PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

MAESTRÍA EN REDES DE COMUNICACIÓN

"Propuesta de un modelo de seguridad para el tratamiento de documentos confidenciales en entidades del estado ecuatoriano que se encuentren sujetas al cumplimiento del acuerdo 166 emitido por la Secretaria Nacional de Administración Pública, caso de estudio Superintendencia de Control del Poder" de Mercado"

Autor

Marcos David Mejía Campoverde

Quito
Diciembre 2015

Director de Tesis
Ing. David Ramírez

AUTORÍA

Yo, **MEJÍA CAMPOVERDE MARCOS DAVID**, portador de la cédula de ciudadanía No. **171087925-3**, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Marcos David Mejía Campoverde
Autor

CERTIFICACIÓN DE AUTORÍA

Yo, **DAVID EDUARDO RAMÍREZ ESPINOSA**, en calidad de Maestrante y Director de la tesis *"Propuesta de un modelo de seguridad para el tratamiento de documentos confidenciales en entidades del estado ecuatoriano que se encuentren sujetas al cumplimiento del acuerdo 166 emitido por la Secretaria Nacional de Administración Pública, caso de estudio Superintendencia de Control del Poder"*, certifico que esta investigación no contiene plagio y es resultado de un trabajo serio desarrollado en su totalidad por el señor ingeniero **MARCOS DAVID MEJÍA CAMPOVERDE.**

David Eduardo Ramírez Espinosa
Director

DEDICATORIA

Ésta tesis es dedicada especialmente a mis padres Anita Campoverde y Luis Hernán Mejía, dos personas que amo profundamente, ya que con su ejemplo me han enseñado valores de lealtad, respeto y responsabilidad; cualidades que las aplico cada día de mi vida y que me han abierto puertas tanto en el campo personal como profesional.

Marcos David Mejía Campoverde

AGRADECIMIENTO

A toda mi familia, padres, hermanos y amigos cercanos por su confianza, paciencia y apoyo constante para la culminación de las metas propuestas.

Al Ing. David Ramírez, por sus consejos y críticas constructivas en la realización del presente proyecto.

Marcos David Mejía Campoverde

ÍNDICE DE CONTENIDOS

1. CAPÍTULO I. 9

1.1. Introducción. 9
1.1. Justificación 10
1.2. Antecedentes 12
1.2. Objetivo general 14
1.3. Objetivos específicos: 14

2. CAPÍTULO II: ESTUDIO DEL ARTE 15

2.1. Seguridad de la información 15
2.2. Amenazas. 15
2.2.1. Tipos de Amenaza. 15
2.2.2. Origen de las Amenazas. 16
2.3. Vulnerabilidades. 16
2.4. Servicios de seguridad 16
2.4.1. No repudio 16
2.4.2. Integridad 17
2.4.3. Confidencialidad 17
2.4.4. Disponibilidad 17
2.5. Planificación de la seguridad 17
2.5.1. Consideraciones legales 18
2.5.2. Planes de acción 23
2.6. Encriptación. 23
2.6.1. Encriptación Simétrica. 23
2.6.2. Encriptación Asimétrica. 24
2.6.3. Autenticación. 25
2.7. Modelos de Autenticación. 26
2.7.1. Contraseñas. 26

2.7.2. Tarjetas inteligentes. 26
2.7.3. Biométrica 27
2.8. Soluciones unificadas de seguridad de la información 27
2.9. Herramienta para evaluación de seguridad 27
2.9.1.1. Hardening.- 32
2.10. Modelos de gestión 32
2.10.1. Organismos de regulación internacional ISO/IEC. 33
2.10.2. ISO/IEC 27000. 33
2.10.3. ISO/IEC 27001 34
2.10.4. ISO 27002-2013 35
2.10.5. Estructura 36
2.10.6. Categorías de seguridad y controles de ISO/IEC 27002 37
2.10.7. ACUERDO 166 46
2.10.7.1. Estructura 46
2.10.7.1.1. Política de seguridad de la información 47
2.10.7.1.2. Organización de la seguridad de la información 48
2.10.7.1.3. Gestión de los activos 48
2.10.7.1.4. Seguridad de los recursos humanos 48
2.10.7.1.5. Seguridad física y del entorno 49
2.10.7.1.6. Gestión de comunicaciones y operaciones 49
2.10.7.1.7. Control de acceso 50
2.10.7.1.8. Adquisición, desarrollo y mantenimiento de sistemas de información 51
2.10.7.1.9. Gestión de los incidentes de la seguridad de la información 51
2.10.7.1.10. Gestión de la continuidad del negocio 52
2.10.7.1.11. Cumplimiento 52
2.11. Información 53
2.12. Tipos de documentos confidenciales en una institución pública ecuatoriana 54
3. CAPÍTULO III: MODELO DE SEGURIDAD PARA EL TRATAMIENTO DE INFORMACIÓN EN ENTIDADES DEL ESTADO ECUATORIANO. 56
3.1. Gestión del modelo de seguridad 56

3.1.1. Criterios generales para la implementación de la gestión de la seguridad. 57
3.1.1.1. Aceptación de las normas por parte de la entidad 58
3.1.1.2. Área de seguridad para el tratamiento de información. 58
3.1.1.2.1. Jefe de seguridad de la información 59
3.1.1.2.2. Analista de Seguridad de la Información 60
3.1.1.3. Actores y responsables sobre el manejo de información. 60
3.1.1.4. Control de acceso a la información 61
3.1.1.4.1. Software de control 61
3.1.1.4.2. Control de acceso 62
3.1.1.4.3. Niveles de acceso 62
3.1.1.4.4. Nivel de consulta de la información 63
3.1.1.4.5. Nivel de mantenimiento de información 63
3.1.1.5. Clasificación de la información. 63
3.1.1.6. Riesgos en la información 64
3.1.1.7. Controles para mitigar riesgos 65
3.1.1.7.1. ¿Quiénes deberían participar? 66
3.1.1.8. Gestión de la cultura 67
3.1.1.9. Gestión de la seguridad 67
3.1.1.10. Lineamientos para seguimiento de la metodología planteada 68
3.1.1.10.1. Planificar (Nivel inicial) 68
3.1.1.10.2. Hacer (implementación y operación).- 69
3.1.1.10.3. Verificar (supervisión y revisión del SGSI) 69
3.1.1.10.4. Actuar (mantenimiento y mejora del SGSI) 69
3.2. Solución técnica para la gestión del modelo de seguridad 69
3.2.1. Infraestructura de Red Informática 69
3.2.2. Conexión a Internet. 70
3.2.3. Administración. 71
3.2.4. Servicios. 71
3.2.5. Infraestructura Virtualizada 71
3.2.6. Propuesta de solución Técnica 71
3.2.7. Herramientas para Monitoreo de red 71

3.2.8. Herramientas para prevención de fuga de información 72
3.2.8.1. Symantec Data Loss Prevention. 72
3.2.8.2. McAfee DLP Endpoint 73
3.2.8.3. Websense DLP 73
3.2.1. Esquema de seguridad. 75
4. CAPÍTULO IV: APLICACIÓN DEL MODELO PROPUESTO PARA LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO (SCPM). 80
4.1. ¿Qué es la Superintendencia de Control del Poder de Mercado? 80
4.1.1. Misión 80
4.1.2. Visión 81
4.1.3. Objetivos estratégicos 81
4.1.4. Estructura organizacional por procesos 82
4.1.4.1. Procesos de la Superintendencia de Control del Poder de Mercado 82
4.1.5. Estructura básica alineada a la misión: 83
4.1.6. Situación actual de tratamiento de información en la SCPM 85
4.1.7. Tipos de documentos que maneja la SCPM. 86
4.1.8. Flujo de documentos con que cuenta la SCPM 86
4.1.9. Documentación externa 88
4.1.10. Documentación interna 90
4.1.11. Archivo de expediente 92
4.1.12. Custodia de expediente 92
4.1.13. Documentación externa pública 93
4.1.14. Documentación externa confidencial 94
4.1.15. Documentación externa secreta 95
4.2. Análisis acerca del estado de infraestructura actual donde reposa la documentación actual que maneja la SCPM 96
4.2.1. Planos de la oficina matriz de la SCPM 96
4.2.2. Esquema de Infraestructura de Red oficina Matriz.- 98
4.2.2.1. Core y Distribución.- 98
4.2.2.2. Acceso.- 99

4.2.3. Detalle de la herramienta Nessus.- 100
4.2.4. Escaneo de Vulnerabilidades Nessus 101
4.2.5. Características técnicas de herramientas de fuga de información 115
4.2.6. Control de acceso físico 118
4.3. Análisis acerca del estado de documentación actual que maneja la SCPM 125
4.4. Modelo para la implementación de documentación para la SCPM 126
4.5. Adopción de buenas prácticas de seguridad de la información 127
4.5.1. Área de seguridad para el tratamiento de información 128
4.5.2. Actores y responsabilidades 129
4.5.3. Controles de acceso 130
4.5.3.1. Control de accesos lógico 130
4.5.4. Clasificación de la información e identificación de activos 133
4.5.4.1. Clasificación y control de información 137
4.5.4.2. Niveles de clasificación. 137
4.6. Evaluación de riesgos 144
4.6.1. Criterios de evaluación del riesgo 144
4.6.2. Criterios de Impacto 144
4.7. Controles a ser implementados 150
4.7.1. Políticas de operación 150
4.7.1.1. Políticas sobre el control de acceso a los sistemas. 150
4.7.1.1.1. Objetivo 150
4.7.1.1.2. Generalidades 150
4.7.1.1.3. Sobre los dispositivos móviles 152
4.7.1.1.4. Métricas 152
4.7.1.1.5. Herramienta 153
4.7.1.2. Políticas acerca del recurso humano. 153
4.7.1.2.1. Objetivos 153
4.7.1.2.2. Generalidades sobre el empleo y contratación 153
4.7.1.2.3. Sobre las responsabilidades de la SCPM. 154
4.7.1.2.4. Conocimiento, educación y capacitación 155
4.7.1.2.5. Sobre la terminación de la relación laboral o cambio de funciones 155

4.7.1.2.6. Métricas 157
4.7.1.3. Política sobre el manejo de información confidencial. 157
4.7.1.3.1. Objetivos 157
4.7.1.3.2. Alcance 157
4.7.1.3.3. Definiciones 158
4.7.1.3.4. Generalidad 158
4.7.1.3.5. Aspectos generales 158
4.7.1.3.6. Sobre el manejo de información en estaciones de trabajo 159
4.7.1.3.7. Proceso de notificación 160
4.7.1.3.8. Medidas disciplinarias 161
4.7.1.3.9. Métricas 161
4.7.1.3.10. Herramienta 161
4.7.2. Documentación 161
5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 163
5.1. Conclusiones. 163
5.2. Recomendaciones. 165
6. BIBLIOGRAFÍA 167

ÍNDICE DE FIGURAS

Capítulo 2
Figura 2.1 Esquema de clave simétrica. 24
Figura 2.2 Esquema de clave asimétrica. 25

Capítulo 3
Figura 3.1 Modelo de seguridad. 57
Figura 3.2 Esquema de personal de seguridad. 59
Figura 3.3 Esquema de red de la SCPM 70
Figura 3.4 Esquema de servicio de red institucional 70
Figura 3.5 Esquema de seguridad de la información propuesto para el presente proyecto 76

Capítulo 4
Figura 4.1 Estructura orgánica funcional de la SCPM. 84
Figura 4.2 Flujo de documentación externa de la SCPM. 89
Figura 4.3 Flujo de documentación interna de la SCPM. 91
Figura 4.4 Flujo de archivo de expediente de la SCPM. 92
Figura 4.5 Flujo custodia de expediente de la SCPM. 93
Figura 4.6 Flujo de documentación externa pública de la SCPM. 94
Figura 4.7 Flujo de documentación externa confidencial de la SCPM. 95
Figura 4.8 Flujo de documentación externa secreta de la SCPM. 96
Figura 4.9 Planos de la oficina Matriz de la SCPM 97
Figura 4.10 Estructura de red SCPM Matriz 98
Figura 4.11 Porcentaje de Afectación del HP Switch 102
Figura 4.12 Porcentaje de Afectación del Firewall 103
Figura 4.13 Vulnerabilidades Servidor de archivos 106
Figura 4.14 Vulnerabilidades de la Wac 110
Figura 4.15 Vulnerabilidades equipos a frontera 114
Figura 4.16 Vulnerabilidades equipo a frontera. 114
Figura 4.17 Vulnerabilidades equipo a frontera 115
Figura 4.18 Vulnerabilidades equipo a frontera 115
Figura 4.19 Esquema de control de documentos SCPM 120
Figura 4.20 Flujo de documentación externa con seguridad 130
Figura 4.21 Manejo de documentos en la SCPM 134
Figura 4.22 Manejo de documentos internos en la SCPM. 135
Figura 4.23 Manejo de trámites externos en la SCPM. 135

ÍNDICE DE TABLAS

Capítulo 2
Tabla 2.1 Cláusulas y categorías de seguridad ISO / IEC 27002 36
Tabla 2.2 Objetivos de control y controles de ISO 27002 38
Tabla 2.3 Cláusulas acuerdo 166 46

Capítulo 3
Tabla 3.1 Cuadro comparativo de soluciones DLP 73

Capítulo 4
Tabla 4.1 Esquema de VLANS SCPM 100
Tabla 4.2 Resumen de Vulnerabilidades equipos SCPM 101
Tabla 4.3 Vulnerabilidades cortafuegos SCPM 102
Tabla 4.4 Vulnerabilidades servidor UIO-SRVFILESERV 103
Tabla 4.5 Vulnerabilidades WAC 106
Tabla 4.6 Vulnerabilidades equipos zonales SCPM 111
Tabla 4.7 Identificación de activos de información 140
Tabla 4.8 Clasificación de la información 143
Tabla 4.9 Ponderación de riesgos 145
Tabla 4.10 Ponderación de impacto 146
Tabla 4.11 Evaluación de riesgos 147

CAPÍTULO I

1.1. Introducción

La presente tesis está compuesta de cinco capítulos, mismos que consideran aspectos de concepto, análisis y propuesta de un modelo de seguridad para el tratamiento de documentación confidencial, ya que en la actualidad cada vez y con más frecuencia se ve la necesidad de resguardar la información de una forma correcta y adecuada.

En el primer capítulo se plantean los antecedentes y objetivos que permiten la elaboración de la presente investigación, exponiendo generalidades que permitieron el incentivo para la elaboración del presente proyecto.

En el segundo capítulo se exponen conceptos y cualidades técnicas que deben ser tomadas en cuenta para cumplir con el objeto de la investigación y que permitirán afianzar la solución propuesta.

En el tercer capítulo se realiza la propuesta del modelo de seguridad que dará tratamiento a los documentos que se denominen confidenciales y sensibles; en el mismo se pretende dar los lineamientos que permitan garantizar un adecuado tratamiento de la información que mantenga un lineamiento correcto con las necesidades institucionales.

Con el tiempo los mecanismos para filtrarse a redes institucionales ha incrementado de forma considerable por lo que en la actualidad hay que considerar muchas más variables que permitan controlar el entorno tecnológico en el que vivimos, por lo que en el cuarto capítulo se realizará la aplicación de la solución propuesta en un caso práctico, mostrando los beneficios que esta investigación propone.

El quinto capítulo se encuentran las conclusiones y recomendaciones que se darán a la Superintendencia de Control del Poder de Mercado tomando en cuenta que es un organismo de control que se dedica a corregir todos los abusos económicos que se enmarcan dentro del estado ecuatoriano; tomando en cuenta que toda la información que se la tramita en interno es muy apreciada por empresas u operadores económicos que pueden considerarse comprometidos con la ley vigente que rige en el Ecuador.

1.1. Justificación

Debido a que la información que maneja, cada entidad es de vital importancia y fundamental se requiere que la misma tenga los debidos controles de acceso y que ésta se encuentre con las características de confidencialidad, integridad, disponibilidad y no repudio establecidas de una forma correcta.

La seguridad es un proceso relevante en la consecución de los objetivos del negocio de toda organización, por lo que se debe identificar de forma correcta cuáles son los activos de la información que deben ser precautelados y contar con todas las garantías de seguridad que intervengan.

La clonación o suplantación de identidad, el robo de información mediante interceptación de mensajes, modificación de mensajes, análisis no permitido de tráfico, suplantación de identidad, conexiones no autorizadas a equipos y servidores, malware, ataques de denegación de servicios, *hackers*[1], *crakers*[2], *sniffers*[3], *spamme*[4]*r*, amenazas de personal interno, se han vuelto métodos comunes y eficaces para poder tener accesos a varias empresas con el fin de obtener información de forma ilícita poniendo en riesgo a todos los activos de la información.

Con todos los eventos generados se considera prudente que toda organización cuente con un modelo de seguridad de la información y más aún en información que es muy sensible y debe ser tratada con toda la responsabilidad del caso.

La Secretaría Nacional de Administración Pública emitió un acuerdo donde dispone a las entidades de la Administración Pública Central, Institucional y que dependan de la Función Ejecutiva el uso obligatorio de las normas técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 [5] para la gestión de seguridad de la Información; ésta norma se tomará como referencia para el planteamiento del modelo

[1] Hackers.- Intrusos que se dedican a la obtención de información a manera de pasatiempo y reto técnico.
[2] Crakers.- Su objetivo es atacar sistemas informáticos de forma ilegal con el objetivo de obtener algún beneficio personal.
[3] Sniffers.- Intrusos que se dedican a rastrear y descifrar mensajes que circulan por una red.
[4] Spammer.- Se dedican al envío de miles de mensajes de correo electrónico no solicitado mediante redes como Internet, con el objetivo de obtener de manera ilegal información de los usuarios, así como también el colapso en los buzones de correo.
Información recurada de: http://es.slideshare.net/mamuga/tipos-de-ataques-y-vulnerabilidades-en-una-red

[5] INEN – ISO/IEC 27000.- Normas técnicas ecuatorianas para la gestión de seguridad de la información. Recuperado de: http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2013/11/NTE_aprobadas_SCT_TIC_2012.pdf

de seguridad propuesto para el presente proyecto, con el afán de regular de una forma adecuada varios aspectos que involucran tratamiento de información, acompañado de tecnología que permita garantizar un control correcto de la misma.

1.2. Antecedentes

De los casos suscitados en Ecuador en cuanto a Delitos Informáticos, de Enero a Diciembre del 2010, se recibieron más de 866 denuncias en diferentes fiscalías del país por delitos tradicionales cometidos por y con mecanismos informáticos, de las cuales 697 fueron apropiación ilícita, 86 denuncias propiamente de delito informático como vulneración a páginas de servicio público, 82 a páginas de servicio privado y 1 por estafa utilizando medios informáticos.

La ausencia de una estructura de políticas, normas y procedimientos ha hecho que las empresas e instituciones tengan fallos en su infraestructura y han sido víctimas de filtraciones de personal externo que han logrado la obtención de información de manera ilícita.

En la actualidad la información es un activo de toda institución y como tal se debe tomar muy en cuenta su protección y tratamiento; es fundamental no menospreciar o minimizar su importancia ya si la información es accedida por personas maliciosas y su uso es inadecuado puede generar un impacto muy fuerte y negativo en las instituciones que sean víctimas de este evento.

En el diario el Universo, el 26 de febrero del 2013 se reportó un caso donde la Fiscalía se encontraba investigando un caso de Piratería informática en un centro de

estudios superior, específicamente comenta del caso sucedido en la Universidad de Especialidades Espíritu Santo (UESS), donde personal externo logró vulnerar su infraestructura y logró poder cambiar calificaciones de un grupo de estudiantes.

Comentan que a pesar de realizar una auditoría de forma general al sistema informático cada período, estas personas tuvieron la habilidad de filtrarse en su red local y cristalizar este objetivo negativo para la institución.

En el Ecuador este delito está tipificado en el artículo 415 numeral 1 del Código Penal, con una pena que va desde los tres hasta los cinco años y una multa desde 200 hasta 600 dólares.

La fiscalía señalo a través de un medio público que este tipo de delitos consisten en "aquellos en donde se vulneran algún sistema, se ingresan a un sistema informático y se extraen datos o se altera la información existente dentro del sistema". Agregó que también que la apropiación indebida de valores económicos de cuentas bancarias (a través de este tipo de filtraciones), también constituye una forma de delito informático.

El diario el Mercurio en su artículo publicado el 22 de noviembre del 2013, y titulado "PIRATERÍA INFORMÁTICA", indican que en declaraciones del estado Ecuatoriano afirman se ha filtrado información desde la computadora del Procurador del Estado, que tiene que ver con el caso Cheron – Texaco, se dice que determinada persona opositara al gobierno ingresó a los correos electrónicos y se hizo de información reservada entre el abogado del Estado y el ejecutivo.

Con lo expuesto se requiere resaltar la importancia de dedicar recursos tecnológicos en la preservación de la seguridad de la información en cualquier entidad o institución.

1.2. Objetivo general

Proponer un modelo de seguridad para tratamiento de información confidencial en entidades del estado ecuatoriano, aplicado como caso de estudio a la Superintendencia de Control del Poder de Mercado.

1.3. Objetivos específicos:

- Establecer una propuesta de modelo de seguridad con los respectivos controles para manejo de información confidencial y que el mismo sea aplicado en entidades del estado ecuatoriano.
- Clasificar la información sensible dentro de una entidad del estado ecuatoriano, para proponer controles y acciones que permitan minimizar el riesgo de fuga de información.
- Proponer un esquema técnico para una empresa del estado ecuatoriano que permita aumentar la seguridad en el tratamiento de información institucional.

CAPÍTULO II: ESTUDIO DEL ARTE

2.1. Seguridad de la información

La seguridad de la información se enfoca en técnicas y características preventivas y reactivas que emplean las organizaciones que buscan para mantener la confidencialidad, disponibilidad e integridad en información.

2.2. Amenazas.

Las amenazas son hechos que pueden producir daños de diversos tipos cuando éstos se activan en un momento en el tiempo.

2.2.1. Tipos de Amenaza.

Los eventos que se clasifican como amenaza pueden ser intencionales o no intencionales:

Intencionales.- se las conoce a aquellas acciones que intentan producir daños o capturar información de manera planificada.

No intencionales.- se las conoce a las acciones que se producen por omisiones y que de manera espontánea resaltan las vulnerabilidades que ponen en riesgo los activos de la información.

2.2.2. Origen de las Amenazas.

El origen de las amenazas pueden verse desde el punto de vista de la entidad que maneja los datos, las mismas pueden generarse por orígenes externos, agresiones técnicas o de origen interno, como la negligencia del propio personal o las condiciones técnicas con que cuenta la institución.

2.3. Vulnerabilidades.

Las vulnerabilidades son aquellas condiciones o capacidades adversas que hace susceptible a una organización a amenazas que pueden producir algún tipo de daño a la información o la integridad de la información.

2.4. Servicios de seguridad

Características de servicios que permiten establecer procedimientos de seguridad dentro de una institución; entre las más comunes se encuentran: no repudio, integridad, confidencialidad y disponibilidad.

2.4.1. No repudio

Se basa principalmente en mantener la continuidad de los servicios, es decir evitar la interrupción del ambiente de producción por cualquier tipo de factor.

Para mantener la continuidad de los servicios hay varias pruebas que permiten el monitoreo y alertas oportunas de éstos eventos.

2.4.2. Integridad

Permite asegurar que no se ha falseado la información, es decir, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación.

2.4.3. Confidencialidad

Capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

2.4.4. Disponibilidad

El sistema se mantiene funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo.

2.5. Planificación de la seguridad

Se define a las estrategias que cada organización emplea para planificar sus acciones en casos donde se detecten o se visualicen amenazas para su red donde se involucren sus activos de información.

2.5.1. Consideraciones legales

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, publicada en el Registro Oficial / Suplemento 557 del 17 de Abril del 2002 tuvo un avance muy importante en el sentido de incluir figuras penales que hagan punibles los ilícitos informáticos con lo cual, junto al Código Penal, integran normas creadas para la Sociedad de la Información.

Dentro de estas normas promulgadas en la Ley 67 posteriormente incluidas al Código Penal, constan los siguientes ilícitos informáticos:

- Art.57 LCEFEMD[6]: **Infracciones informáticas.-** Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.
- Art.58 LCEFEMD, Conc. Art.202.1 CP: **Contra la Información Protegida**.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

[6] **LCEFEMD.-** Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

- Art.58 últ.inc LCEFEMD, Conc. Art.202.2 CP: **Obtención y utilización no autorizada de información.-** La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.
- Art.59 LCEFEMD, Conc. Art.262 CP: **Destrucción Maliciosa de Documentos.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos,

títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

- Art.60 LCEFEMD, Conc. Art.353.1 CP: **Falsificación electrónica.-** Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:
    1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
    2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
    3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
- Art.61 LCEFEMD, Conc. Art.415.1 CP: **Daños informáticos**.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los

programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

- Art.61 últ.inc LCEFEMD, Conc. Art.415.1 CP: **Destrucción de instalaciones para transmisión de datos.-** Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.
- Art.62 LCEFEMD, Conc. Art.553.1 CP: **Apropiación ilícita**.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta

o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

- Art.62 últ.inc LCEFEMD, Conc. Art.553.2 CP: **Pena.-** La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:
    1. Inutilización de sistemas de alarma o guarda;
    2. Descubrimiento o descifrado de claves secretas o encriptadas;
    3. Utilización de tarjetas magnéticas o perforadas;
    4. Utilización de controles o instrumentos de apertura a distancia; y,
    5. Violación de seguridades electrónicas, informáticas u otras semejantes.
- Art.63 LCEFEMD, Conc. Art.563 inc.2 CP: **Estafa. -** Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.
- Art.64 LCEFEMD, Conc. Art.606.20 CP: Violación Derecho a la Intimidad.- Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

2.5.2. Planes de acción

Son documentos que deben estar debidamente aprobados para que en caso de contingencia éstos sean aplicados como protocolos establecidos.

2.6. Encriptación.

La aparición de la Informática y el uso masivo de las comunicaciones digitales, han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas, y por tanto, la seguridad de esta información debe garantizarse. Este desafío ha generalizado los objetivos de la criptografía para ser la parte de la criptología que se encarga del estudio de los algoritmos, protocolos (se les llama protocolos criptográficos), y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

2.6.1. Encriptación Simétrica.

La encriptación simétrica[7] se basa en la generación de una clave única que debe ser conocida y recibida por el emisor y el receptor del mensaje como se muestra en la **Figura 2.1**.

[7] Encriptación simétrica. Recuperado de: http://4esobglr.blogspot.com/2013/05/tipos-de-encriptados.html

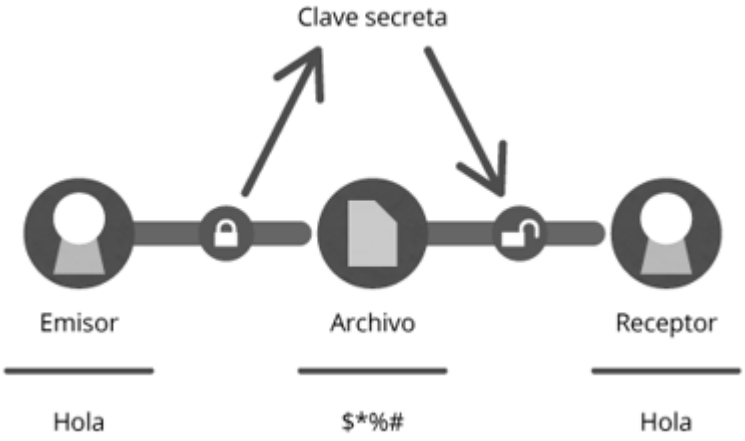

Figura 2.1 **Esquema de clave simétrica.**

Fuente: http://4esobglr.blogspot.com/2013/05/tipos-de-encriptados.html

2.6.2. Encriptación Asimétrica.

La encriptación asimétrica[8] se basa en la generación de una clave pública y una clave secreta, la clave pública puede ser difundida para que llegue a un grupo de receptores, pero la clave privada sólo sabe el receptor que confirme su identidad, tal como se muestra en la **Figura 2.2**.

[8] Encriptación asimétrica. Recuperado de: http://4esobglr.blogspot.com/2013/05/tipos-de-encriptados.html

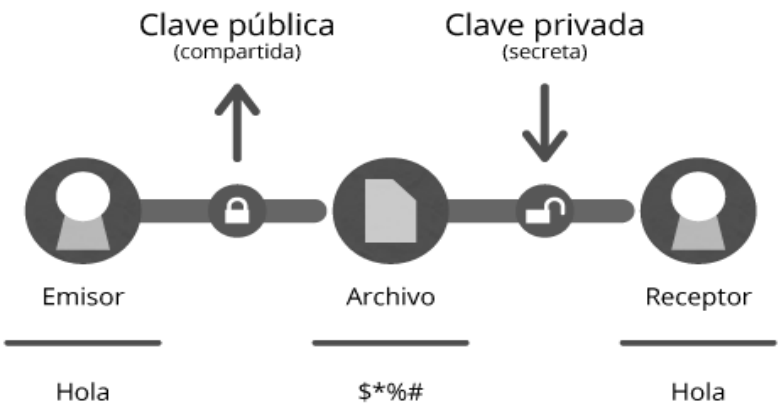

Figura 2.2 **Esquema de clave asimétrica.**

Fuente: http://4esobglr.blogspot.com/2013/05/tipos-de-encriptados.html

2.6.3. Autenticación.

Es la propiedad que permite identificar si la generación de la información que es recibida pertenece al emisor que indica ser, es decir se pretende evitar la suplantación de identidad.

La comprobación de la identidad es un tema primordial en el manejo de seguridad de la información, si manejamos esta variable de manera correcta estamos estableciendo un protocolo correcto para manipulación de la información.

En la actualidad se han creado varios sitios que suplantan la identidad de cuentas de usuario, y al parecer tan reales, se pueden filtrar en cualquier ambiente institucional que no tenga una validación de esta acción.

2.7. Modelos de Autenticación.

La autenticación es un método que sirve para dar seguridad a cualquier evento que requiera la afirmación de acceso a cualquier usuario. Si esta información es captada o suplantada por terceras personas el riesgo que se genera en cualquier organización es muy grande. Existen modelos de autenticación como los siguientes:

2.7.1. Contraseñas.

La contraseña es un método de autenticación que consiste en admitir el ingreso a un sitio cualquiera, mediante la digitación de caracteres que sólo deben ser conocidos por el usuario que indica que está accediendo al sitio[9].

2.7.2. Tarjetas inteligentes.

La tarjeta inteligente es un método de autenticación que contiene en su espacio físico un micro chip que almacena información del dueño del servicio[10].

[9] Contraseña. Método de autenticación. Recuperado de: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=185

[10] Tarjeta inteligente. Método de autenticación. Recuperado de: http://www.upm.es/institucional/Estudiantes/OrdenacionAcademica/CarneUniversitario/e58f4105a0052210VgnVCM10000009c7648aRCRD

2.7.3. Biométrica

Es un método de autentificación donde intervienen rasgos físicos de la persona, es decir un usuario puede autenticarse a través de su huella digital, reconocimiento facial, iris del ojo, etc[11].

2.8. Soluciones unificadas de seguridad de la información

La protección de la información es el problema más crítico con que debe tratar cualquier entidad u organización, ya que con el tiempo se han creado nuevos métodos para extracción de la misma, volviendo a las empresas vulnerables frente a éstas posibles amenazas.

El presente proyecto se encuentra enfocado a la propuesta de un modelo de seguridad acompañado de políticas, técnicas y herramientas tecnológicas desde una óptica de seguridad de la información, por lo que a continuación se presentan alternativas que ayudarían a la consecución de este objetivo.

2.9. Herramientas para evaluación de seguridad

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, integridad, disponibilidad y no repudio de la misma.

[11] Biométrica. Método de autenticación. Recuperado de: http://dis.um.es/~lopezquesada/documentos/IES_1112/SAD/curso/UT3/ActividadesAlumnos/grupo7/Enlaces/BIOMETRICO.html

Lo que se pretende es contar con un respaldo tecnológico que permita la aplicación de técnicas y políticas que actúen como escudo para el ingreso no autorizado de personas ajenas a la institución.

Parte de los mecanismos pueden ser Humanos y Tecnológicos. Entre los Tecnológicos se puede enfocar en la prevención de falla de Hardware y/o Software, fallas en sistemas de acceso, fallas en ataques de virus informáticos, etc. En lo que se refiere a la parte Humana, se debe manejar el control referente a un posible hurto de información, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crakers, hackers, robo de contraseñas, suplantación de identidad, alteraciones, etc. Éstos controles deben ser acompañados de herramientas que permitan realizar éstas acciones de supervisión.

Las herramientas tecnológicas son un complemento de seguridad para el esquema con que cuenta cada entidad. Las seguridades informáticas deben estar apoyadas con políticas que respalden el uso de las mismas y que las mantengan amparadas en un resguardo jurídico.

Es muy importante contar con el respaldo de las personas que se encuentran a cargo de cada institución y realizar contar con un esquema que permita dar el tratamiento adecuado a los esquemas de seguridad propuestos.

Se recomienda contar con un oficial de seguridad que permita realizar los lineamientos que se ajusten a la realidad institucional y que puedan ser contralados con herramientas tecnológicas.

Como parte del presente proyecto se pretende realizar un análisis de la situación actual con que cuenta la Superintendencia de Control del Poder de Mercado con el afán de tener una visión más clara de su esquema actual y poder realizar recomendaciones de seguridad acompañados de políticas que respalden un Sistema de Gestión de Seguridad de la Información propuesto para el tratamiento de información confidencial.

Basados en lo expuesto anteriormente, existen herramientas que permiten realizar un análisis de las vulnerabilidades como parte de las medidas ejecutadas para protección de la información, entre las más destacadas existen analizadores de vulnerabilidades, herramientas para análisis de protocolos de red y herramientas para prevención de fuga de información.

A continuación se realizará un resumen de sus funcionalidades y cuál es objeto de cada una:

2.9.1. Analizador de vulnerabilidades.-

También conocidos como "analizadores de red", son herramientas que permiten escanear redes, con el objeto de detectar posibles vulnerabilidades luego del análisis de los puertos abiertos en un equipo específico o en toda la red. El proceso de análisis utiliza solicitudes que permiten determinar los servicios que se están ejecutando en un host remoto. Gracias a la estructura de los paquetes TCP/IP recibidos, el escáner de seguridad puede identificar, a veces, qué sistema operativo está utilizado en el equipo remoto, así como las versiones de las

aplicaciones asociadas con los puertos. Para este procedimiento las herramientas lanzan todo un arsenal de paquetes que serán transmitidos por los puertos abiertos que posteriormente emitirán una respuesta por parte del servidor dando a conocer si existe un error o no. Una vez identificado el riesgo de seguridad, es muy probable que el mismo sea utilizado para acciones que no estén contempladas dentro del marco legal de la institución.

Existen varias herramientas que permiten analizar las vulnerabilidades de una red como por ejemplo: Snort, Nessus, Ethereal, etc.

En el presente proyecto se pretende realizar un escaneo de éste tipo, que permita corregir las vulnerabilidades que se encuentren luego del mismo. Permitirá tener una visión mucho más clara de la red y como se pueden corregir las vulnerabilidades encontradas.

2.9.2. Analizador de protocolos de red.-

Un analizador de protocolos es una herramienta que sirve para desarrollar y depurar protocolos y aplicaciones de red. Permite la captura de diversas tramas para analizarlas, ya sea en tiempo real o después de haberlas capturado. Por analizar se entiende que el programa puede reconocer que la trama capturada pertenece a un protocolo concreto (TCP, ICMP...) y muestra al usuario la información decodificada. Una vez identificado el riesgo de seguridad, es muy probable que el mismo sea utilizado para acciones que no estén contempladas dentro del marco legal de la institución.

Existen varias herramientas que permiten analizar los protocolos de red como por ejemplo: Nmap, Nessus, TCPDump, etc.

En el presente proyecto se pretende realizar un análisis de este tipo con el afán de corregir las vulnerabilidades encontradas. Todas las observaciones o correcciones deben estar acompañadas de políticas que respalden el incremento de controles o actualización de políticas a ser implementadas.

2.9.3. Prevención de fuga de información (DLP).-

Son herramientas que permiten la identificación, supervisión y protección de datos en movimiento y datos estáticos, a través de inspecciones de contenido, análisis de contexto de seguridad de una forma centralizada; Las herramientas están diseñadas para detectar y prevenir el uso no autorizado y la transmisión no autorizada de información confidencial. Las directivas de DLP son paquetes sencillos que contienen conjunto de condiciones, compuestos por reglas de transporte, acciones y excepciones que se crean en el centro de administración para poder ejercer control dentro de un objetivo establecido. En la actualidad hay varias herramientas con diferentes características que ayudan al tratamiento de información en este sentido como por ejemplo DLP McAfee, DLP Symantec, SAS DLP, etc.

Las herramientas de prevención de fuga de información permitirán aplicar políticas de supervisión en sitios estratégicos donde se alojará información catalogada como confidencial y mantendrá una alerta constante en el caso de

ejecutarse una actividad atípica a la que normalmente se gestiona por los procesos internos.

2.9.4. Hardening[12].-

La intención del hardening es fortalecer la seguridad informática, ejecutando acciones y procedimientos que impidan el acceso fácil por personas no autorizadas; se debe hacer la vida difícil al atacante para poder acceder a la red. Su propósito es entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

Hay que tener claro que el Hardening no forjará equipos invulnerables, pero si reforzará de manera significativa la seguridad implementada.

Este procedimiento de Hardening es un complemento adicional para las herramientas de evaluación de seguridad informática.

2.10. Modelos de gestión

Un modelo de gestión permite establecer un enfoque y un marco de referencia objetivo, riguroso y estructurado para el diagnóstico de una organización, así como determinar las líneas de mejora continua hacia las cuales deben orientarse los esfuerzos de la misma. Existen modelos que en la actualidad

[12] Hardening.- En seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades. Recuperado de: http://blog.smartekh.com/%C2%BFque-es-hardening/

ya son utilizados en varias empresas y son tomados como referencia para la implementación de buenas prácticas en procesos de seguridad de la información.

2.10.1. Organismos de regulación internacional ISO/IEC.

*"*El estándar ISO/IEC tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en el año de 1995. Este documento hace referencia a las normas de seguridad o buenas prácticas que deben tomar en cuenta las instituciones que manejan información sensible y que requieren contar con un sistema de seguridad para el acceso a la información.

Tras un período de revisión y actualización en el año 2005 se realiza una nueva publicación del documento, saliendo la versión ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007*"* (The ISO 27000 Directory, 2013).

Luego de éstos eventos se ha conseguido que la publicación de ésta documentación se extienda a nivel mundial para poder mantener estándares de seguridad que ayuden a las organizaciones a mitigar los riesgos que implica el ingreso no deseado a información institucional que se considera un activo para las organizaciones.

2.10.2. ISO/IEC 27000.

*"*El estándar ISO/IEC tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en el año de 1995. Este documento hace referencia

a las normas de seguridad o buenas prácticas que deben tomar en cuenta las instituciones en general; la aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite interpretaciones de conceptos técnicos y de gestión.

Luego de éstos eventos se ha conseguido que la publicación de ésta documentación se extienda a nivel mundial para poder mantener estándares de seguridad que ayuden a las organizaciones a mitigar los riesgos que implica el ingreso no deseado a información institucional que se considera un activo para las organizaciones.

2.10.3. ISO/IEC 27001

Tras un período de revisión y actualización en el año 2005 se realiza una nueva publicación del documento, saliendo la versión ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007" (The ISO 27000 Directory, 2013).

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las normas ISO/IEC 27000 [13]son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO[14]) y la Comisión Electrotécnica Internacional (IEC[15]) (The ISO 27000 Directory, 2013), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

2.10.4. ISO 27002-2013

ISO /IEC 27002, es un estándar internacional no certificable, que proporciona una guía de buenas prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información (ISO/IEC, 2005). Forma parte de la serie ISO/IEC 27000, preparada por el comité ISO/IEC JTC 1/SC 27 para la Seguridad de la Información que incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información

[13] ISO/IEC 27000. Normas de estándares de seguridad. Recuperado de: http://www.iso27002.es/

[14] ISO. Organización internacional para la estandarización. Recuperado de: http://www.iso.org/iso/home.html

[15] IEC. Comisión electrónica internacional. Recuperado de: http://std.iec.ch/glossary

2.10.5. Estructura.

El estándar ISO /IEC 27002 contiene 11 cláusulas de control de seguridad, las cuales colectivamente contienen un total de 39 categorías de seguridad es principales y una cláusula introductoria que representa la evaluación y tratamiento del riesgo.

Las cláusulas y el número de categorías de seguridad principales de cada una se muestra en la **Tabla 2.1**:

Tabla 2.1 **Cláusulas y categorías de seguridad ISO / IEC 27002. (ISO 27002)**

CLÁUSULA	NÚMERO DE CATEGORÍAS DE SEGURIDAD
Política de Seguridad	1
Organización de la Seguridad de la Información	2
Gestión de activos	2
Seguridad de recursos humanos	3
Seguridad física y ambiental	2
Gestión de comunicaciones y operaciones	10
Control de acceso	7
Adquisición, desarrollo y mantenimiento de Sistemas de Información	6
Gestión de incidentes de seguridad de la información	2
Gestión de la continuidad comercial	1
Conformidad	3

2.10.6. Categorías de seguridad y controles de ISO/IEC 27002[16]

Cada categoría de seguridad contiene un objetivo que establece lo que se debiera lograr, y uno o más controles que se pueden aplicar para lograr el objetivo de control. El estándar contempla un total de 133 controles.

Cada control a su vez está definido con un enunciado específico para satisfacer el objetivo de control, el lineamiento de implementación del control y de manera opcional información que puede estar relacionada con aspectos legales u otros estándares.

En la **Tabla 2.2** se resume cada una de las cláusulas con sus respectivas categorías, caracterizadas por su objetivo de control y sus controles.

[16] ISO/IEC 27002. Controles del Sistema de Gestión de Seguridad de la Información. http://www.iso27000.es/download/ControlesISO27002-2013.pdf

Tabla 2.2 **Objetivos de control y controles de ISO 27002. (ISO 27002)**

CLÁUSULA	CATEGORÍA / OBJETIVO DE CONTROL	CONTROL
5. POLÍTICA DE SEGURIDAD	5.1 Política de seguridad de la información	5.1.1 Documento de la política de seguridad de la información
		5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna	6.1.1 Compromiso de la Dirección con la seguridad de la información.
		6.1.2 Coordinación de la seguridad de la información.
		6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
		6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
		6.1.5 Acuerdos de confidencialidad
		6.1.6 Contacto con las autoridades.
		6.1.7 Contacto con grupos de especial interés
		6.1.8 Revisión independiente de la seguridad de la información
	6.2 Terceros	6.2.1 Identificación de los riesgos derivados del acceso de terceros.
		6.2.2 Tratamiento de la seguridad en la relación con los clientes

		6.2.3 Tratamiento de la seguridad en contratos con terceros
7. GESTIÓN DE ACTIVOS	7.1 Responsabilidad sobre los activos	7.1.1 Inventario de activos
		7.1.2 Propiedad de los activos.
		7.1.3 Uso aceptable de los activos.
	7.2 Clasificación de la información	7.2.1 Directrices de clasificación
		7.2.2 Etiquetado y manipulado de la información
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	8.1 Antes del empleo.	8.1.1 Funciones y responsabilidades
		8.1.2 Investigación de antecedentes.
		8.1.3 Términos y condiciones de contratación.
	8.2 Durante el empleo	8.2.1 Responsabilidades de la Dirección.
		8.2.2 Concienciación, formación y capacitación en seguridad. de la información
		8.2.3 Proceso disciplinario
	8.3 Cese del empleo o cambio de puesto de trabajo.	8.3.1 Responsabilidad del cese o cambio
		8.3.2 Devolución de activos
		8.3.3 Retirada de los derechos de acceso
9. SEGURIDAD FÍSICA Y DEL ENTORNO	9.1 Áreas seguras.	9.1.1 Perímetro de seguridad física.
		9.1.2 Controles físicos de entrada
		9.1.3 Seguridad de oficinas, despachos e instalaciones
		9.1.4 Protección contra las amenazas externas y de origen ambienta
		9.1.5 Trabajo en áreas seguras

		9.1.6 Áreas de acceso público y de carga y descarga
	9.2 Seguridad de los equipos	9.2.1 Emplazamiento y protección de equipos.
		9.2.2 Instalaciones de suministro.
		9.2.3 Seguridad del cableado
		9.2.4 Mantenimiento de los equipos.
		9.2.5 Seguridad de los equipos fuera de las instalaciones.
		9.2.6 Reutilización o retirada segura de equipos.
		9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	10.1 Responsabilidades y procedimientos de operación.	10.1.1 Documentación de los procedimientos de operación
		10.1.2 Gestión de cambios
		10.1.3 Segregación de tareas
		10.1.4 Separación de los recursos de desarrollo, prueba y operación.
	10.2 Gestión de la provisión de servicios por terceros.	10.2.1 Provisión de servicios
		10.2.2 Supervisión y revisión de los servicios prestados por terceros.
		10.2.3 Gestión del cambio en los servicios prestados por terceros
	10.3 Planificación y aceptación del sistema	10.3.1 Gestión de capacidades
		10.3.2 Aceptación del sistema.

	10.4 Protección contra el código malicioso y descargable.	10.4.1 Controles contra el código malicioso
		10.4.2 Controles contra el código descargado en el cliente
	10.5 Copias de seguridad	10.5.1 Copias de seguridad de la información
	10.6 Gestión de la seguridad de las redes.	10.6.1 Controles de red
		10.6.2 Seguridad de los servicios de red
	10.7 Manipulación de los soportes	10.7.1 Gestión de soportes extraíbles
		10.7.2 Retirada de soportes
		10.7.3 Procedimientos de manipulación de la información
		10.7.4 Seguridad de la documentación del sistema.
	10.8 Intercambio de información.	10.8.1 Políticas y procedimientos de intercambio de información.
		10.8.2 Acuerdos de intercambio.
		10.8.3 Soportes físicos en tránsito
		10.8.4 Mensajería electrónica
		10.8.5 Sistemas de información empresariales.
	10.9 Servicios de comercio electrónico	10.9.1 Comercio electrónico
		10.9.2 Transacciones en línea
		10.9.3 Información públicamente disponible
	10.10 Supervisión.	10.10.1 Registros de auditoría.
		10.10.2 Supervisión del uso del sistema.

		10.10.3 Protección de la información de los registros.
		10.10.4 Registros de administración y operación.
		10.10.5 Registro de fallos.
		10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.	11.1 Requisitos de negocio para el control de acceso.	11.1.1 Política de control de acceso.
	11.2 Gestión de acceso de usuario	11.2.1 Registro de usuario
		11.2.2 Gestión de privilegios.
		11.2.3 Gestión de contraseñas de usuario
		11.2.4 Revisión de los derechos de acceso de usuario
	11.3 Responsabilidades de usuario	11.3.1 Uso de contraseñas
		11.3.2 Equipo de usuario desatendido
		11.3.3 Política de puesto de trabajo despejado y pantalla
	11.4 Control de acceso a la red.	11.4.1 Política de uso de los servicios en red
		11.4.2 Autenticación de usuario para conexiones externas
		11.4.3 Identificación de los equipos en las redes
		11.4.4 Protección de los puertos de diagnóstico y configuración remotos
		11.4.5 Segregación de las redes
		11.4.6 Control de la conexión a la red
		11.4.7 Control de encaminamiento (routing) de red.

	11.5 Control de acceso al sistema operativo	11.5.1 Procedimientos seguros de inicio de sesión
		11.5.2 Identificación y autenticación de usuario
		11.5.3 Sistema de gestión de contraseñas.
		11.5.4 Uso de los recursos del sistema
		11.5.5 Desconexión automática de sesión
		11.5.6 Limitación del tiempo de conexión.
	11.6 Control de acceso a las aplicaciones y a la información	11.6.1 Restricción del acceso a la información.
		11.6.2 Aislamiento de sistemas sensibles.
	11.7 Ordenadores portátiles y teletrabajo	11.7.1 Ordenadores portátiles y comunicaciones móviles.
		11.7.2 Teletrabajo
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	12.1 Requisitos de seguridad de los sistemas de información.	12.1.1 Análisis y especificación de los requisitos de seguridad.
	12.2 Tratamiento correcto de las aplicaciones	12.2.1 Validación de los datos de entrada
		12.2.2 Control del procesamiento interno
		12.2.3 Integridad de los mensajes.
		12.2.4 Validación de los datos de salida.
	12.3 Controles criptográficos.	12.3.1 Política de uso de los controles criptográficos
		12.3.2 Gestión de claves
	12.4 Seguridad de los archivos de sistema	12.4.1 Control del software en explotación.
		12.4.2 Protección de los datos de prueba del sistema

		12.4.3 Control de acceso al código fuente de los programas
	12.5 Seguridad en los procesos de desarrollo y soporte	12.5.1 Procedimientos de control de cambios
		12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
		12.5.3 Restricciones a los cambios en los paquetes de software
		12.5.4 Fugas de información
		12.5.5 Externalización del desarrollo de software.
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Control de las vulnerabilidades técnicas
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	13.1 Notificación de eventos y puntos débiles de seguridad de la información	13.1.1 Notificación de los eventos de seguridad de la información
		13.1.2 Notificación de puntos débiles de seguridad.
	13.2 Gestión de incidentes y mejoras de seguridad de la información	13.2.1 Responsabilidades y procedimientos
		13.2.2 Aprendizaje de los incidentes de seguridad de la información
		13.2.3 Recopilación de evidencias
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
		14.1.2 Continuidad del negocio y evaluación de riesgos
		14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información

		14.1.4 Marco de referencia para la planificación de la continuidad del negocio
		14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad
15. CUMPLIMIENTO.	15.1 Cumplimiento de los requisitos legales.	15.1.1 Identificación de la legislación aplicable
		15.1.2 Derechos de propiedad intelectual (DPI)
		15.1.3 Protección de los documentos de la organización
		15.1.4 Protección de datos y privacidad de la información de carácter personal
		15.1.5 Prevención del uso indebido de recursos de tratamiento de la información
		15.1.6 Regulación de los controles criptográficos
	15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico	15.2.1 Cumplimiento de las políticas y normas de seguridad.
		15.2.2 Comprobación del cumplimiento técnico
	15.3 Consideraciones sobre las auditorías de los sistemas de información.	15.3.1 Controles de auditoría de los sistemas de información.
		15.3.2 Protección de las herramientas de auditoría de los sistemas de información

2.10.7. ACUERDO 166

El acuerdo 166 [17] es una publicación emitida por la Secretaría Nacional de Administración Pública, donde se emiten directrices prioritarias para Gestión de Seguridad de la Información donde se pretende iniciar un proceso de mejora continua en las instituciones de la Administración Pública del estado Ecuatoriano. Cabe recalcar que el EGSI no reemplaza la norma INEN ISO/IEC 27002 [18] sino que marca como prioridad la implementación de algunas directrices que ayudarían a incrementar la seguridad de la información en las entidades públicas, así como la confianza de los ciudadanos en la administración pública.

2.10.7.1. Estructura

El acuerdo 166 está compuesto por 11 cláusulas de control de seguridad de la información, que intentan guiar a las entidades del estado a un estado de seguridad eficiente para sus operaciones diarias.

A continuación en la **Tabla 2.3** se presenta un resumen de las cláusulas que contiene el documento:

Tabla 2.3 **Cláusulas acuerdo 166. Elaborado por Autor**

Nro.	CLÁUSULA
1	Política de seguridad de la información
2	Organización de la seguridad de la información
3	Gestión de los activos

[17] Acurdo 166. Norma de seguridad de la Información para entidades del estado ecuatoriano. Recuperado de: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2013/11/Acuerdo-No.-1661.pdf

[18] INEN ISO/IEC 27002. Normas de gestión de seguridad de la Información. Recuperado de: http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2013/11/NTE_aprobadas_SCT_TIC_2012.pdf

4	Seguridad de los recursos humanos
5	Seguridad física y del entorno
6	Gestión de comunicaciones y operaciones
7	Control de acceso
8	Adquisición, desarrollo y mantenimiento de sistemas de información
9	Gestión de los incidentes de la seguridad de la información
10	Gestión de la continuidad del negocio
11	Cumplimiento

2.10.7.1.1. Política de seguridad de la información

La política de seguridad de la información indica que "Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

2.10.7.1.2. Organización de la seguridad de la información

Establece normas y lineamientos internos para la difusión, capacitación y sensibilización de las políticas de seguridad que se generen en la institución.

Ésta organización debe involucrar la participación y cooperación de los cargos directivos de la institución.

La organización de la seguridad de la información deberá estar manejada oficialmente por el Comité de Gestión de seguridad de la Información.

2.10.7.1.3. Gestión de los activos

Establece normas y lineamientos internos para el manejo e inventario de activos institucionales. En ésta Gestión se indica que debe incluirse el inventario de Hardware, Software, redes.

También se hace mención y énfasis en la asignación de un responsable de los activos que se manejen en la institución, su uso aceptable y como deben estar identificados.

En resumen la Gestión de los activos indica lineamientos para el correcto uso y manipulación de los activos institucionales.

2.10.7.1.4. Seguridad de los recursos humanos

Indica la necesidad de verificar a los candidatos, previa su contratación.

En la etapa de contratación se debe realizar la entrega formal de funciones y responsabilidades al funcionario que ingresa a la Institución, así como también informar al Oficial de Seguridad

acerca de las actividades para que éstas sean evaluadas y monitoreadas en el caso que amerite.

2.10.7.1.5. Seguridad física y del entorno

Se debe evaluar el estado de la seguridad física, con la definición de perímetros de seguridad. Las mismas deben contar con la fortaleza necesaria para impedir el ingreso de personas ajenas a la institución.

La Institución debe contar con equipamiento adecuado contra incendio y puertas de evacuación debidamente monitoreadas que cumplan con normas nacionales e internacionales.

Este control también hace referencia al control de acceso físico e identificación adecuada a sitios catalogados como críticos dentro de la Institución.

2.10.7.1.6. Gestión de comunicaciones y operaciones

Se menciona que todos los procedimientos de operación deben estar debidamente documentados, sean éstos manejo de información, respaldo y restauración de información, servicios de procesamiento de datos, manejo de errores, manejo de incidentes, manejo de medios e informes especiales, procedimientos para la eliminación segura de tareas fallidas, procedimientos para reinicio y recuperación del sistema en caso de fallas y registros de auditoría de la información de registro del sistema.

Indica que los cambios que se generen en operaciones deben estar debidamente documentados, evaluar el impacto y contar con la aprobación y contingencia en el caso que se presente.

Se menciona la importancia de la separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción, así como la importancia del monitoreo y revisión de los servicios de manera permanente.

2.10.7.1.7. Control de acceso

Se menciona la importancia del control de acceso de los usuarios a los sistemas de información, asegurando identidad para evitar intrusión no autorizada.

Se debe tener un registro de los usuarios que ingresan a los sistemas informáticos estableciendo un procedimiento formal, documentado y difundido que evidencie detalladamente los pasos y responsables.

Se deben gestionar debidamente los privilegios a través de un proceso formal de autorización, los mismos deben tener el nivel adecuado y justo para que el usuario final pueda trabajar sin problemas.

Se debe levantar un registro de los servicios de la red institucional y asignar permisos de acceso a cada usuario y grupo de usuarios que utilizan este servicio.

2.10.7.1.8. Adquisición, desarrollo y mantenimiento de sistemas de información

Hace referencia a la forma de mantener activa los sistemas de información con que cuenta cada institución, en esta parte se debe definir los requerimientos de seguridad como criptografía, control de sesiones, etc.

Se debe tomar en cuenta la validez de los datos de entrada y que los mismos se encuentren direccionados de manera segura hacia un ambiente que se destine para este fin; se debe llevar un registro de todos los movimientos o actividades implicadas en el proceso de entrada de datos.

Otra parte importante es mantener la integridad de la información en todas sus etapas, la información debe permanecer íntegra desde el inicio de procesamiento hasta su salida.

La confidencialidad de la información se debe garantizar, para esto se debe documentar quienes deben tener acceso y uso y cuál es su alcance en el tratamiento de manipulación y acceso a la información.

Se recomienda implementar un sistema de administración de claves cifradas y que las mismas se encuentren protegidas contra copia o divulgación no autorizada.

2.10.7.1.9. Gestión de los incidentes de la seguridad de la información

En esta parte se gestiona y analiza los incidentes sobre los eventos de seguridad reportados; se debe instaurar un

procedimiento formal para reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.

Se debe identificar el incidente, registrarlo y notificar al oficial de seguridad para que se encargue de darle el seguimiento y tratamiento adecuado al caso que se identifique.

Todos los empleados, contratistas y usuarios de terceras partes deberán informar sobre estos asuntos a su director o directamente a su proveedor de servicio tan pronto sea posible.

La debida gestión establece responsabilidades, las cuáles deben ser ejecutadas dependiendo de la criticidad del caso.

2.10.7.1.10. Gestión de la continuidad del negocio

Debe existir un responsable designado como coordinador de la continuidad de los servicios institucionales (continuidad del negocio), éste debe identificar los procesos críticos para prevenir a las autoridades y corregir cualquier eventualidad presentada.

2.10.7.1.11. Cumplimiento

El cumplimiento de la gestión debe estar amparada con la legislación aplicable, para lo cual se recomienda tener inventariada todas las normas legales, estatutarias, reglamentarias y contractuales.

Se debe precautelar la protección de datos y privacidad de la información personal; precautelar el uso inadecuado de servicios de procesamiento de información.

2.11. Información

La información es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado. Toda empresa u organización genera y mantiene información, misma que conlleva al objeto de su misión y objetivos empresariales.

Existen varios tipos de información, entre las cuales destacan:

Información interna.- Es la información que circula al interior de una empresa u organización. Busca llevar un mensaje para mantener la coordinación entre los distintos departamentos, permite la introducción, difusión y aceptación de pautas para el desarrollo organizacional.

Información externa.- Es la información que ingresa en una empresa u organización, generada por diferentes vías externas, esta información debe ser seleccionada ya que no siempre es de utilidad para los fines de la empresa.

Información pública.- Es la información que todas las personas tienen derecho a conocerla y solicitarla en caso que lo requieran. Ésta información debe estar expuesta de manera ágil y transparente.

Información confidencial.- Es la información que no debe estar expuesta para el público en general y debe ser tratada sólo por personal autorizado a la misma. Ésta información debe estar resguardada y tratada por criterios de seguridad como la confidencialidad, integridad, disponibilidad y no repudio.

2.12. Tipos de documentos confidenciales en una institución pública ecuatoriana

En la Ley Orgánica de Transparencia y Acceso a la Información Pública se establecen parámetros para acceso a los documentos basándose en principios generales.

El acceso a la información pública es un derecho de las personas que garantiza el estado.

Existen varios tipos de documentos que ingresan a las instituciones, los mismos deben ser clasificados según su nivel y grado de afectación a los intereses institucionales.

Todas las entidades que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, implementarán, según sus competencias y posibilidades presupuestarias, programas de difusión y capacitación dirigidos tanto a los servidores públicos, como a las organizaciones de la sociedad civil, con el objeto de garantizar una mayor y mejor participación ciudadana en la vida del Estado.

Para que la documentación llegue a un estado de difusión pública debe pasar por un proceso de tratado y clasificación de la misma.

En todas las instituciones del estado ecuatoriano se debe manejar un registro de todos los documentos que se clasifiquen como confidenciales y darles un tratamiento adecuado en todo su proceso de trámite.

Para el caso de estudio la Superintendencia de Control del Poder de Mercado cuenta con documentos de trámite general, pero también con documentos como denuncias de operadores económicos, resoluciones de casos,

información de allanamientos, etc., cada uno debe ser tratado según corresponda y debe estar apegado a las normas institucionales vigentes.

CAPÍTULO III: MODELO DE SEGURIDAD PARA EL TRATAMIENTO DE INFORMACIÓN EN ENTIDADES DEL ESTADO ECUATORIANO.

3.1. Gestión del modelo de seguridad

La información que es elaborada y generada por los procesos de las instituciones es un activo, que como otros bienes, tienen gran valor y necesita ser protegida en forma apropiada. El modelo de Seguridad de la Información protege dicha información de una amplia gama de amenazas, con el fin de asegurar la continuidad de los procesos institucionales y la entrega de productos y servicios a usuarios / clientes/ beneficiarios, minimizando el daño de la institución y maximizando la eficiencia y las oportunidades de la mejora de la gestión organizacional.

La presente propuesta de modelo de seguridad se basa en los conceptos del acuerdo 166 emitido por la Secretaría Nacional de Administración Pública para la seguridad de la información, la misma que proporciona un conjunto de información filtrada y actualizada que refuerza los conceptos de seguridad de la información del marco principal, haciendo uso de otros estándares como la norma ISO/IEC 27002.

Los conceptos presentados en el acuerdo 166 para la seguridad de la información, al igual que otros marcos de referencia o estándares, no pretenden ser una guía prescriptiva para las necesidades de todas las empresas e instituciones; por lo tanto, el modelo que se presenta a continuación corresponde a una adaptación de las necesidades y priorización de las partes interesadas en la seguridad de la información de los sistemas que manejan las instituciones del estado ecuatoriano, considerando las cláusulas que intervienen en el acuerdo 166 y las que se presentan en conjunto con la norma ISO/IEC 27002 detalladas en el capítulo 2.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

3.1.1. Criterios generales para la implementación de la gestión de la seguridad.

Los criterios que a continuación se detallan en la **Figura 3.1**, tratan de describir las principales fases que se requieren para un modelo de seguridad que se ajuste a las necesidades institucionales en base al acuerdo 166 emitido por la Secretaría Nacional de Administración Pública y la norma ISO/IEC 27002, para el tratamiento de información en entidades del estado ecuatoriano.

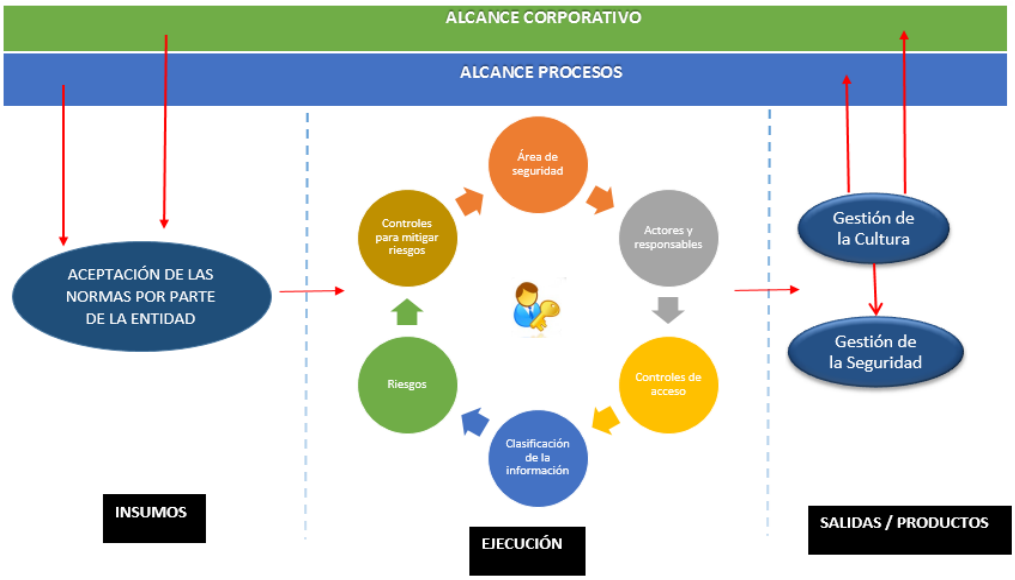

Figura 3.1 **Modelo de seguridad. Elaborado por autor**

3.1.1.1. Aceptación de las normas por parte de la entidad

Es de suma importancia que las partes interesadas dirijan y soporten las iniciativas de seguridad de la información, con el objetivo de asegurar que las prácticas sean logradas y sostenidas. Bajo este mismo criterio, se debe solicitar desde un inicio, la aprobación de las iniciativas por parte de las partes interesadas relevantes, demostrando que las necesidades de estas están siendo tomadas en cuenta.

En esta etapa se debe presentar la iniciativa de seguridad a las autoridades de la institución, para que se acepten las normas propuestas en el modelo descrito como se indica en la **Figura 3.1** ya que son parte de los insumos de entrada.

En el ámbito de la seguridad de la información, la adopción de estándares y buenas prácticas, debe mantener compatibilidad con un marco de gestión de riesgos institucional. Este requerimiento garantizará que las buenas prácticas puedan integrarse con otros métodos o prácticas más generales que se utilicen a nivel corporativo, es decir que se aprovechará la ventaja brindada por la estandarización al permitir ampliar las prácticas y procedimientos de forma natural e independiente de la plataforma tecnológica.

3.1.1.2. Área de seguridad para el tratamiento de información.

Se debe adoptar la recomendación de las buenas prácticas de seguridad de la información; cada entidad debe contar con un área de seguridad que se maneje de manera independiente, pero que tenga el aval

de la máxima autoridad para poder desempeñar de manera autónoma acciones que permitan mitigar riesgos de pérdida o fuga de información.

El área de seguridad deberá estar conformada por 2 roles principales, el Jefe de seguridad de la Información y el Analista de seguridad de la información agrupado bajo 2 actividades principales, de acuerdo al esquema de la **Figura 3.2**:

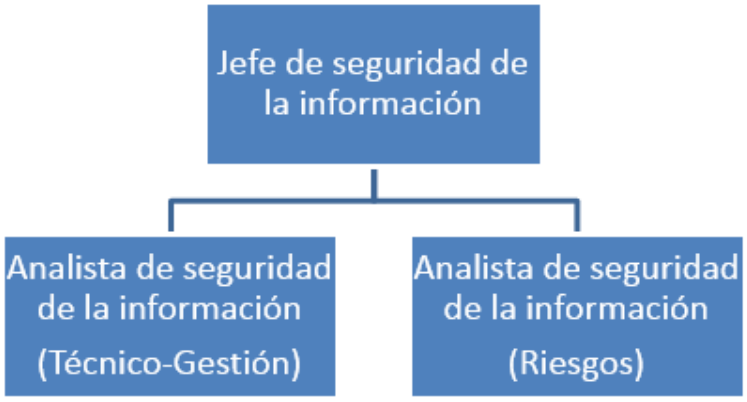

Figura 3.2 **Esquema de personal de seguridad. Elaborado por autor.**

3.1.1.2.1. Jefe de seguridad de la información

Definir, mantener y controlar políticas, procesos, procedimientos y estándares de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la información.

Funciones y responsabilidades:

- Definir y comunicar la estrategia de seguridad de la información alineada con la estrategia institucional.
- Controlar el cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información.

- Formular y mantener el plan de contingencia de seguridad que garantice la disponibilidad, confidencialidad e integridad de la información.

3.1.1.2.2. Analista de Seguridad de la Información

Aplicar las políticas, procesos, procedimientos y estándares definidos en el sistema de gestión de seguridad de la información para garantizar la integridad, disponibilidad y confidencialidad de la información.

Funciones y responsabilidades:

- Evaluar los riesgos de seguridad de la información y proponer acciones a incluirse en el Plan de Seguridad de la Información.
- Gestionar los accesos a los servicios tecnológicos institucionales.
- Participar en la implementación del plan de seguridad de la información.
- Monitorear e informar acerca del cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información.

3.1.1.3. Actores y responsables sobre el manejo de información.

Considerada la información como un activo institucional, ésta debería ser justificada y siempre tener asignado un propietario.

Se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos.

El término "propietario" identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona disponga de los derechos de propiedad reales del activo.

3.1.1.4. Control de acceso a la información

Algunos usuarios o extraños (personal no autorizado) pueden encontrar alguna forma mediante la cual, logren el acceso al sistema o la base de datos de las instituciones y descubrir información clasificada o datos no autorizados. Para este evento se deberá considerar la existencia de:

3.1.1.4.1. Software de control

Deben existir programas protegidos que mantengan y controlen a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

El uso de tal programa puede conferir al usuario algunos de los privilegios que corresponden al control de dichos programas. La transferencia de privilegios es adecuada si el programa actúa como filtro de la información.

3.1.1.4.2. Control de acceso

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.

La identificación de un usuario debe ser muy difícil de imitar y copiar. Aunque su nombre pueda ser único, es fácil que cualquiera que observe a quienes tienen acceso al sistema lo copie.

La responsabilidad del manejo de la clave corresponde exclusivamente al usuario que en su momento recibió esta autorización de ingreso.

Las claves de acceso deben tener un grado de dificultad para que las mismas no puedan ser copiadas o grabadas de manera fácil.

En toda institución es recomendable que el responsable de cada área asigne y actualice en forma periódica la clave asignada a los usuarios.

3.1.1.4.3. Niveles de acceso

Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

3.1.1.4.4. Nivel de consulta de la información

El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos, o del Sistema de otro usuario para lograr el acceso.

La autorización de lectura permite leer pero no modificar la información expuesta.

3.1.1.4.5. Nivel de mantenimiento de información

El concepto de mantenimiento de la información consiste en:

- **Ingreso.-** Permite el ingreso de nueva información, pero no la alteración de datos ya existentes.
- **Actualización.-** Permite la actualización de información, pero no la eliminación de datos existentes.
- **Borrado.-** Permite la eliminación de información.

Un usuario puede tener asignados todos, ninguno o una combinación de los accesos a la información.

La autoridad de accesibilidad es la que se le da al administrador de la información, que entre otras cosas puede autorizar la creación de nuevos usuarios, acceso a cierto tipo de módulos o información, bloqueo o limitación de accesos, etc.

3.1.1.5. Clasificación de la información.

Por el tipo de información que ingresa y se genera en las instituciones, ésta debe ser clasifica de manera adecuada para poder brindarle un tratamiento correcto acorde a las leyes y normas internas vigentes.

El propósito de esta acción es proteger los activos de información con que cuenta cada institución.

Se consideran activos de la información a los siguientes elementos:

- **La información** propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- **Los equipos/sistemas/infraestructura** que soportan esta información y que tienen acceso a los sistemas que manejan cada institución.
- **Las personas** que utilizan la información y que tiene el conocimiento de los procesos institucionales.

Se debe clasificar la información para indicar la necesidad, prioridades y nivel de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

3.1.1.6. Riesgos en la información

Sin adecuadas medidas de seguridad las instituciones pueden estar expuestas a no sólo la destrucción de la información física, sino también de la destrucción de la infraestructura tecnológica que almacena la información lógica.

La destrucción de la infraestructura tecnológica puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Cuando un evento de pérdida de información se concreta por cualquier motivo, es un riesgo para el desempeño normal de la institución que ha sufrido este evento.

Para evitar daños mayores al ser destruida la información, se debe crear respaldos periódicos de la misma y almacenarse en lugares adecuadamente preparados para ese fin, de preferencia en un lugar lejano de donde se encuentran los equipos que usualmente lo manejan.

Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal que no cuenta con principios de ética y que se han involucrado en el rol institucional. Por ejemplo: hay casos en los que, funcionarios que han sido recientemente despedidos o están enterados que ellos van a ser despedidos, han destruido o modificado archivos para su beneficio inmediato o futuro.

La revelación o infidencia es otra forma que se puede presentar en un escenario institucional con funcionarios que buscan sacar provecho de la información que se genera dentro de cada entidad y que no debe ser expuesta a terceras personas que para que puedan aprovecharse de la misma.

3.1.1.7. Controles para mitigar riesgos

Dado que el objeto que motiva la creación de estos lineamientos es la salvaguarda de los datos y la información generada, los presentes

lineamientos deberán ser observados por las autoridades que conforman las instituciones.

El empleo de métricas para medir, monitorear y reportar la efectividad y eficiencia de los controles de seguridad de información, así como las políticas de seguridad de información es una tarea continua que debe desarrollar el área de seguridad de información en cada institución.

Adicionalmente, el monitoreo permite realizar los cambios que sean necesarios, dado que los sistemas de información y recursos de información constantemente cambian.

El área de seguridad de información debe contar con un proceso de revisión periódica de las métricas, reportándose cualquier actividad inusual que se presente.

3.1.1.7.1. ¿Quiénes deberían participar?

Debe formarse un grupo de personas de las diferentes áreas dentro del alcance del SGSI, entre ellos:

a. Comité de Seguridad de la Información: Gestionará los recursos necesarios con las autoridades de cada institución y guiará prioridades en función de las políticas y lineamientos establecidos en su momento por el área de seguridad.
b. Equipo de Planeamiento de la Seguridad de la Información: Estimará recursos, propondrá alternativas técnicas y planes de implementación en un alto nivel, en particular para aquellos controles y objetivos de control relacionados.
c. Representantes de las áreas directamente afectadas.
d. Representantes del área de Tecnología.

e. Representantes de Talento Humano.
f. Representantes de la Seguridad Física.
g. Dueños de los procesos y activos afectados (estratégicos y operacionales).

De la participación de ésta representación debería salir la siguiente documentación:

a. Plan de Implementación de Controles (cronograma, responsable / equipo, etc.)
b. Registro y Documentación de las actividades y controles implementados

3.1.1.8. Gestión de la cultura

Una vez implementada la etapa de ejecución se debe motivar a la institución para que se cultive la iniciativa de Gestión de cultura, en esta etapa se debe socializar y gestionar en interno para que el modelo se cumplido y ejecutado de manera óptima. Ésta debe tener un alcance corporativo y de procesos para que tenga éxito y pueda mantenerse vigente.

3.1.1.9. Gestión de la seguridad

Se debe tener en cuenta que la seguridad es un tema que debe ser tratado de manera permanente; el presente modelo es una propuesta que garantizará el manejo de seguridad de la información de manera

oportuna para tener respuestas frente a incidentes o casos de posible fuga de información.

3.1.1.10. Lineamientos para seguimiento de la metodología planteada

Se ha definido como estrategia para la implementación del modelo de seguridad de la información, la implementación de lineamientos planteados en el ciclo de PHVA el cual está alineado con la familia de estándares ISO/IEC 27000.

Los lineamentos de seguridad de la información basados en la norma internacional ISO/IEC 27001:2005 adoptan un enfoque por proceso para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de los sistemas de gestión de la seguridad de la Información.

Esta norma internacional proporciona un modelo robusto para implementar los principios de dichas directrices que rigen la evaluación de riesgos, el diseño y la implementación de la seguridad, así como la gestión y la reevaluación de la seguridad.

El ciclo PHVA se lo describe con las siguientes etapas: Planear, Hacer, Verificar y Actuar.

3.1.1.10.1. Planificar (Nivel inicial)

En esta etapa se pretende definir las políticas, objetivos, procesos, y procedimientos relevantes para gestionar el riesgo y mejorar la seguridad de la información, adoptando los lineamientos aplicables, con el fin de obtener resultados acordes con las políticas y objetivos institucionales.

3.1.1.10.2. Hacer (implementación y operación).-

Etapa de implementación y operación de políticas, controles, procesos y procedimientos para la implementación de controles de seguridad de la información.

3.1.1.10.3. Verificar (supervisión y revisión del SGSI)

Etapa para evaluar y medir el rendimiento de los procesos y políticas implementadas, así como también es la etapa para informar de los resultados.

3.1.1.10.4. Actuar (mantenimiento y mejora del SGSI)

Etapa donde se adoptan medidas correctivas y preventivas, en función de los resultados, para lograr la mejora continua del modelo de seguridad planteado.

3.2. Solución técnica para la gestión del modelo de seguridad

La solución técnica propone establecer controles informáticos en base a debilidades que se encuentren dentro de la red informática con que cuenta la Superintendencia de Control del Poder de Mercado.

A continuación se presentará el esquema actual con que cuenta la SCPM

3.2.1. Infraestructura de Red Informática

La red de la SCPM se encuentra conformada por un esquema que actualmente brinda servicios institucionales a todas sus oficinas a nivel nacional como se muestra en la **Figura 3.3**.

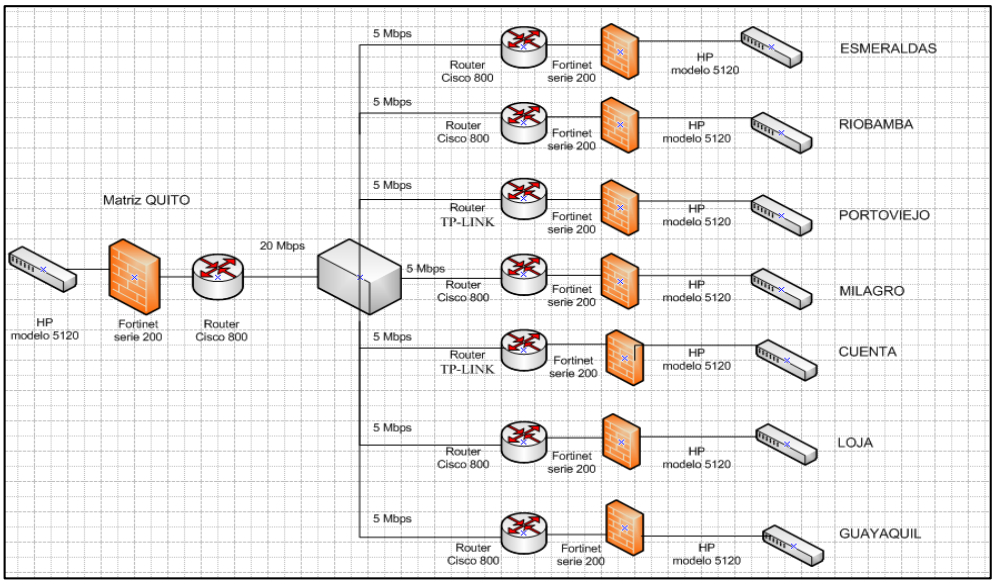

Figura 3.3 **Esquema de red de la SCPM. Elaborado por autor.**

3.2.2. Conexión a Internet.

La SCPM cuenta con un servicio de Internet de 22Mbps contratado con una empresa del estado ecuatoriano. El mismo sirve a toda la oficina matriz y oficinas zonales.

Adicional cuenta con un enlace de respaldo de 5Mbps que sirve en caso de contingencia. Este enlace se encuentra contratado con una empresa privada para garantizar el servicio por diferentes nodos de conexión.

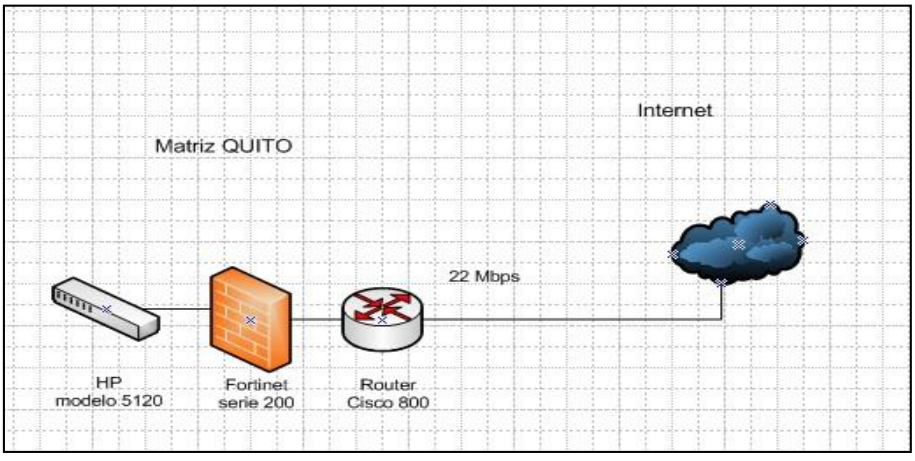

Figura 3.4 **Esquema de servicio de red institucional. Elaborado por autor.**

3.2.3. Administración.

La administración de las redes LAN de la matriz y sucursales se encuentran a cargo de la Dirección de Infraestructura Tecnológica y Comunicaciones de la SCPM y así garantizar un correcto funcionamiento

3.2.4. Servicios.

La SCPM tiene centralizados los servicios de Telefonía IP, Video conferencia e Internet que son administrados desde la Matriz ubicada en Quito y proporcionados hacia las oficinas zonales del país.

3.2.5. Infraestructura Virtualizada

La SCPM cuenta con una infraestructura de virtualización que permite el manejo y administración de sus servidores hacerlo de una manera óptima.

3.2.6. Propuesta de solución Técnica

Para el tratamiento de la información confidencial se considera el apoyo técnico de herramientas tecnológicas que permitan garantizar la operatividad correcta en el SGSI propuesto.

En este sentido se debe realizar un análisis de la situación de infraestructura de red actual desde su parte interna como también a su acceso externo.

3.2.7. Herramientas para Monitoreo de red

Mientras que un sistema de detección de intrusos monitorea una red por amenazas del exterior (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Existen varias herramientas que pueden cumplir con este objetivo, en este sentido se ha tomado en cuenta la herramienta de monitoreo Nessus.

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes

3.2.8. Herramientas para prevención de fuga de información

Para poder establecer un análisis de la herramienta que se ajusta a las necesidades que requiere la Superintendencia de Control del Poder de Mercado, se ha realizado un análisis de las siguientes soluciones que permitirán corregir los problemas con que actualmente cuenta la institución.

3.2.8.1. Symantec Data Loss Prevention[19].

Herramienta que permite detectar en qué lugar de los entornos móviles, la nube e instalaciones se encuentran almacenados los datos institucionales; permite supervisar como están siendo utilizados los mismos para protegerlos de robo dentro y fuera de la red institucional.

[19] Symantec Data Loss Prevention.- Herramienta de seguridad utilizada para la prevención de fuga de información. Recuperado de: http://www.symantec.com/es/mx/data-loss-prevention/

Esta herramienta permite detectar, supervisar y proteger la información que se encuentra dentro de una red institucional.

3.2.8.2. McAfee DLP Endpoint[20]

Solución que ofrece una protección frente al robo y divulgación accidental de los datos confidenciales. Esta protección afecta a todas las redes, las aplicaciones y los dispositivos de almacenamiento extraíbles.

Esta herramienta permite detectar, supervisar y proteger la información que se encuentra dentro de una red institucional.

3.2.8.3. Websense DLP[21]

Permite descubrir y proteger datos confidenciales en la nube o en sitio. Permite asegurar datos personales y de propiedad intelectual, así como también aplicación de políticas personalizadas para adaptarse a necesidades institucionales.

Esta herramienta permite detectar, supervisar y proteger la información que se encuentra dentro de una red institucional.

Tabla 3.1 **Cuadro comparativo de soluciones DLP. Elaborado por autor.**

	McAfee	Symantec	Websense
Auditoria y Reportes Centralizados en cumplimiento para diferentes módulos y/o grupos	100%	100%	100%
Despliegue y Administración Centralizada	100%	50%	50%

[20] McAfee DLP Endpoint.- Herramienta de seguridad utilizada para la prevención de fuga de información. Recuperado de: http://www.mcafee.com/es/products/dlp-endpoint.aspx

[21] Websense.- Herramienta de seguridad utilizada para la prevención de fuga de información. Recuperado de: http://es.websense.com/content/module-dlp.aspx?intcmp=nav-mm-products-module-dlp

Políticas unificadas para DIM[22], DAR[23] y DIU[24]	100%	100%	100%
Monitoreo y Captura por Puerto/Protocolo	100%	50%	50%
Capturar, Monitoreo y Descubrimiento de lo Desconocido	100%	0%	0%
Administración Robusta de casos de Flujo de Trabajo	100%	100%	50%
Descubrimiento de Datos no Estructurados (Network y EndPoint)	100%	50%	50%
Data Discovery estructurado con Registro de Datos Dinámicos.	100%	50%	50%
Ajuste y Validación de Reglas en Tiempo Real	100%	0%	0%
Integración de Contenido Cifrado en DIU, DIM y DAR	100%	50%	50%
Aplicación de Políticas cuando los EndPoints estén Conectados/Desconectados	100%	50%	100%
Integración con DRM[25] para Remediación Automatizada	100%	50%	50%
Integración con Directorio Activo	100%	100%	100%

[22] DIM – Data in Motion.- término que se utiliza para referirse a los datos que atraviesan dentro o fuera de una red. (Email, MSN, Web) – Recuperado de: http://www.victormiranda.com.mx/vmwp/tabla-comparativa-de-dlp/#sthash.wIbKuaKX.dpuf

[23] DAR - Data At Rest.- término que se utiliza para referirse a todos los datos contenidos en Equipos de almacenamiento, que residen en la memoria del Equipo para leer, modificar o cargar.(Todo archivo contenido en un Desktop, Laptop, Servidor o SAN) – Recuperado de: http://www.victormiranda.com.mx/vmwp/tabla-comparativa-de-dlp/#sthash.wIbKuaKX.dpuf

[24] DIU - Data In Use.- término que se utiliza para referirse a los datos que se está leyendo o trabajando en ese momento. (Copiar, Pegar, Imprimir, Abrir; en algún dispositivo de almacenamiento) – Recuperado de: http://www.victormiranda.com.mx/vmwp/tabla-comparativa-de-dlp/#sthash.wIbKuaKX.dpuf

[25] DRM - Digital Rigths Management.- término para las tecnologías de control de acceso, que son utilizados por fabricantes de hardware, los editores, los titulares de derechos de autor y los individuos para limitar el uso de contenidos digitales y dispositivos. – Recuperado de: http://www.victormiranda.com.mx/vmwp/tabla-comparativa-de-dlp/#sthash.wIbKuaKX.dpuf

Como se muestra en la **Tabla 3.1,** existe una herramienta que cumple con todas las características que requiere la solución en el esquema de protección propuesto.

3.2.1. Esquema de seguridad.

Para el tratamiento de la información confidencial se considera el esquema propuesto en la **Figura 3.5,** la misma consta de tres capas que son: servidor, intermedia y clientes.

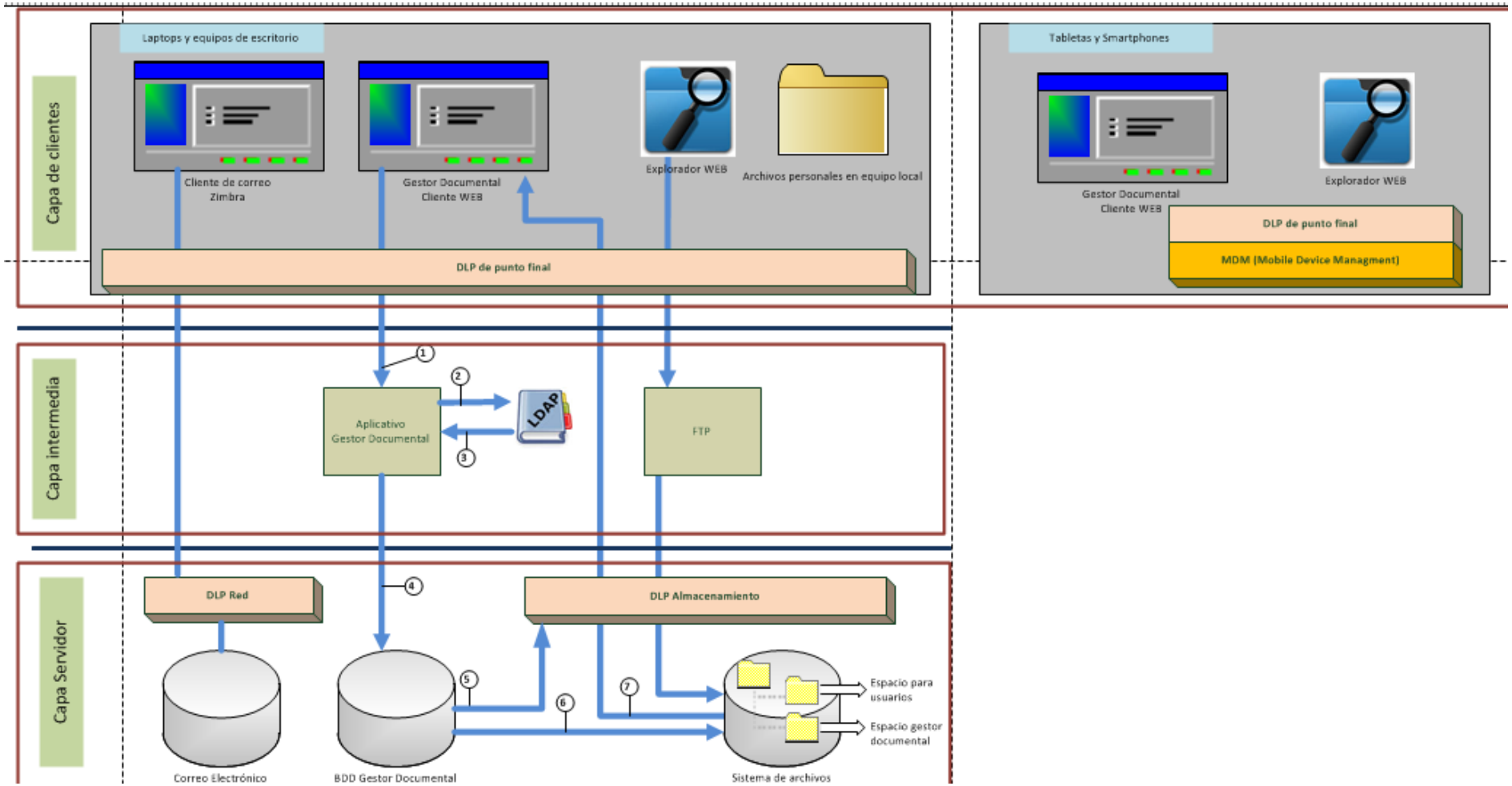

Figura 3.5 **Esquema de seguridad de la información propuesto para el presente proyecto. Elaborado por autor.**

Capa de servidor

Pretende alojar de manera independiente los servidores involucrados en el alojamiento de la información a ser procesada y resguardada. Esto con el fin de mantener un solo ambiente seguro y con direccionamiento IP totalmente independiente y aislado de la red normal que maneja la SCPM.

En el mismo se encontrará alojado el servidor de correo, servidor de bases de datos (que maneje el Gestor Documental Institucional) y el sistema de archivos. Se han tomado como referencia éstos servidores ya que en ellos se alojará información catalogada como sensible. En los mismos se utilizarán herramientas de apoyo de seguridad para monitorear los eventos que se generen en los mismos a cada momento. Se tienen previsto la colocación de un DLP de red y un DLP para los servidores de almacenamiento.

El DLP de red se encargará del monitoreo de tráfico que exista dentro de la institución y mostrará alertas oportunas en el caso de registrarse alguna actividad atípica a la que normalmente se genera en la red institucional.

El DLP para los servidores de almacenamiento actuarán en base a las políticas internas generadas para resguardo de información; el mismo gestionará y controlará todas las posibles alternativas que se utilicen para fuga de información, mantendrá un registro de eventos que ayudarán al oficial de seguridad a tener una reacción rápida y oportuna en el caso de presentarse cualquier actividad atípica y que sea considerada como sospechosa. La herramienta permitirá el monitoreo por usuario con lo cual se crearán responsabilidades sobre la cuenta que se encuentre involucrada actividades sospechosas (en caso de existirlas).

El sistema de archivos contendrá un espacio para información de usuarios y otro espacio para la información que almacene el gestor documental, con esta acción se delimitará claramente qué tipo de información es la que reposa en el sistema de archivos.

Capa de Intermedia

Pretende manejar de manera independiente los aplicativos que se encuentren manipulando flujos de información; para este caso el Gestor Documental y un servidor FTP que servirán para tratamiento y repositorio de la misma. En esta capa también se debe contar con la ayuda de la herramienta para prevención de fuga de información, ya que la misma debe contener en sus políticas, detalles de los mecanismos para prevenir la mala manipulación de la información. Se requiere que la herramienta sea manejada de manera autónoma por el oficial de seguridad ya que al tratarse de información sensible debe estar administrada por el oficial de seguridad designado por la Institución.

En esta capa también se supervisará la información que repose en el servidor FTP, ya que el mismo también va a trabajar como repositorio de información.

El oficial de seguridad es la única persona encargada de validar y notificar los eventos o alertas que se generen del monitoreo constante de éstos repositorios.

Capa de Clientes

Pretende mantener el control de todos los dispositivos de usuario final que van a manipular los aplicativos que manejan información dentro de la institución.

En la capa de cliente serán controlados los accesos a los aplicativos que van a manipular información institucional. Para poder tener acceso todos los usuarios deben cumplir con parámetros de autenticación y acceso limitado para que pueda ejercer solamente sus funciones encomendadas, es decir ningún usuario puede contar con permisos superiores a los que requiere su perfil laboral. Para usuarios críticos se monitoreará de manera permanente los flujos que conllevan la ejecución de su trabajo. Esta capa es de suma importancia ya que la misma puede ser susceptible a la manipulación inapropiada de los usuarios finales.

Con la herramienta y políticas establecidas se controlará el acceso y flujo de información de una manera adecuada evitando adulteración, fraude, modificación, revelación, pérdida, sabotaje en un mayor porcentaje que la situación actual.

La información será tratada de una manera adecuada y contará con mayores fortalezas para su tratamiento y resguardo. En todos los niveles existirá monitoreo permanente de la herramienta de prevención de fuga de información con el afán de contar con un mejor esquema de tratamiento de seguridad de la información.

CAPÍTULO IV: APLICACIÓN DEL MODELO PROPUESTO PARA LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO (SCPM).

4.1. ¿Qué es la Superintendencia de Control del Poder de Mercado?

Mediante Ley Orgánica publicada en el Registro Oficial Suplemento 555 de 13 de octubre de 2011 se crea la Superintendencia de Control del Poder de Mercado, como un organismo técnico de control con capacidad sancionatoria, de administración desconcentrada, con personalidad jurídica, patrimonio propio y autonomía administrativa, presupuestaria y organizativa.

Fue creada para evitar, prevenir, corregir, eliminar y sancionar el abuso de operadores económicos con poder de mercado; la prevención, prohibición y sanción de acuerdos colusorios y otras prácticas restrictivas; el control y regulación de las operaciones de concentración económica; y la prevención, prohibición y sanción de las prácticas desleales, buscando la eficiencia en los mercados, el comercio justo y el bienestar general y de los consumidores y usuarios, para el establecimiento de un sistema económico social, solidario y sostenible.

4.1.1. Misión

"Controlar el correcto funcionamiento de los mercados, previniendo el abuso de poder de mercado de los operadores económicos nacionales y extranjeros y todas aquellas prácticas contrarias a la competencia que vayan en perjuicio de los consumidores, a fin de construir con competitividad y eficiencia el bienestar general de la sociedad". *(Superintendencia de Control del Poder de Mercado, 2015)*

4.1.2. Visión

"Ser una institución modelo con estándares de excelencia en la gestión de la defensa de la competencia, referente de eficiencia, transparencia, control y ética tanto a nivel nacional como internacional generando impactos positivos permanentes en la economía del país, corrigiendo progresivamente las prácticas de los operadores económicos que sean contrarias a la ley, de una manera solvente en lo técnico y jurídico, con la participación de una amplia red conformada por la sociedad civil y la academia." *(Superintendencia de Control del Poder de Mercado, 2015)*

4.1.3. Objetivos estratégicos

- Promover la competencia, la transparencia y eficiencia de los mercados como herramientas hacia el buen vivir.
- Prevenir, controlar y disminuir el abuso del poder de mercado, de los acuerdos y prácticas restrictivas, contrarias al régimen previsto en la ley.
- Controlar las operaciones de concentración económica de acuerdo a lo previsto en la Ley.
- Controlar la existencia de prácticas desleales en el mercado y velar por la lealtad y el desarrollo de las actividades económicas.
- Brindar asesoramiento y apoyo a las unidades de la SCPM en materia de planificación, jurídica, comunicacional, administrativa, financiera, talento humano, documental y tecnológica.

4.1.4. Estructura organizacional por procesos

La estructura organizacional de la Superintendencia de Control del Poder de Mercado, se alinea con su misión y se sustenta en la filosofía y enfoque de productos, servicios y procesos, con el propósito de asegurar su ordenamiento orgánico.

4.1.4.1. Procesos de la Superintendencia de Control del Poder de Mercado

Los procesos que elaboran los productos y servicios de la Superintendencia de Control del Poder de Mercado, se ordenan y clasifican en función de su grado de contribución o valor agregado al cumplimiento de la misión institucional.

Los procesos gobernantes orientan la gestión institucional a través de la formulación de políticas y la expedición de normas e instrumentos para mantener operativa a la Institución.

Los procesos que agregan valor generan, administran y controlan los productos y servicios destinados a usuarios externos y permiten cumplir con la misión institucional, denotan la especialización de la misión consagrada en la Ley y constituyen la razón de ser de la institución.

Los procesos habilitantes están encaminados a generar productos y servicios para los procesos gobernantes, agregadores de valor y para sí mismos, viabilizando la gestión institucional.

Los procesos desconcentrados, encaminados a generar productos y servicios directamente a los clientes externos, en áreas geográficas establecidas, contribuyendo al cumplimiento de la misión institucional.

4.1.5. Estructura básica alineada a la misión:

La Superintendencia de Control del Poder de Mercado, para el cumplimiento de su misión, objetivos y responsabilidades, desarrolla procesos internos y está conformado por procesos agregadores de valor, procesos habilitantes de asesoría y procesos habilitantes de apoyo tal como se muestra en la **Figura 4.1**.

Para el presente proyecto y por tratarse de un tema de seguridad de la información nos centraremos en el tratamiento de información que se genera en los procesos agregadores de valor, ya que en los mismos se asume que se generaría la información sensible que debe protegerse dentro de la Superintendencia de Control del Poder de Mercado.

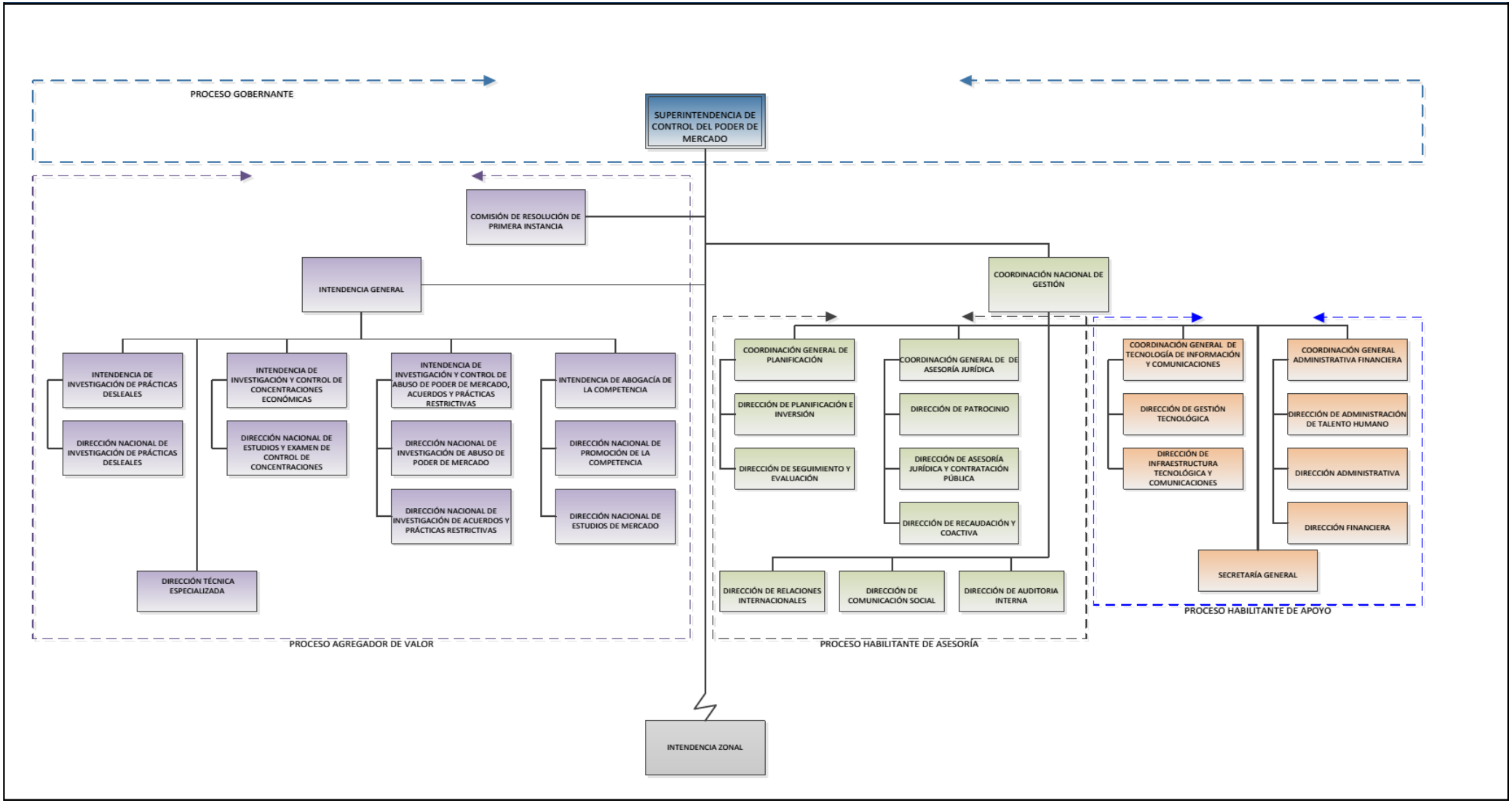

Figura 4.1 **Estructura orgánica funcional de la SCPM. (SCPM, 2015)**

Fuente: http://www.scpm.gob.ec/wp-content/uploads/2015/05/a1-organigrama-de-la-instituci%C3%B3n-SCPM-ABRIL-2015.pdf

4.1.6. Situación actual de tratamiento de información en la SCPM

Dentro de las atribuciones expresas, especiales y específicas de la Superintendencia de Control del Poder de Mercado, se incluye el requerir a los operadores económicos o a las instituciones u órganos del sector público y privado informes, información o documentación relevante que puede ser de carácter confidencial o reservado conforme la naturaleza de la información en los términos de la Constitución y la Ley. Adicionalmente existen procesos propios de esta Superintendencia cuya información es de carácter reservado, como por ejemplo los documentos generados en los procesos previos a la investigación y en la fase de investigación, para lo cual se toman en cuenta las siguientes consideraciones:

a. La clasificación de la información está relacionada con la etapa procesal, así un mismo documento puede ser confidencial durante la realización de una investigación y convertirse en público al final de la misma.
b. Existen documentos que deben estar disponibles solamente para un área de la Institución.

A fin de garantizar la confidencialidad de los documentos digitales de la Superintendencia de Control del Poder de Mercado, es necesario reorganizar los procedimientos con que actualmente cuenta la institución, ya que no existe una organización correcta en lo referente a los mecanismos para prevención de fuga de información.

4.1.7. Tipos de documentos que maneja la SCPM.

La Superintendencia de Control del Poder de Mercado maneja los siguientes tipos de Documentos:

- Resoluciones
- Recomendaciones
- Oficio
- Oficio Circular
- Memorando
- Memorando Circular
- Informe
- Providencia
- Notificación
- Norma técnica

4.1.8. Flujo de documentos con que cuenta la SCPM

La SCPM cuenta con un Gestor Documental, en donde se ingresan algunos documentos (a discreción de personal de la Dirección de Secretaria General ya que no existe una directriz interna), al realizar este ingreso se genera una hoja de ruta, en la misma se formaliza la constancia de la recepción del documento a todos los destinatarios. El aplicativo cuenta con las diferentes características:

- En la Institución no se ha realizado un análisis de seguridad acerca de los documentos confidenciales que se manejan en la misma.

- La Institución no cuenta con la documentación de diseño de la aplicación que maneja los documentos confidenciales.
- No se cuenta con el diagrama de entidad relación de la base de datos
- La aplicación no considera permisos de seguridad para acceso a la información clasificada como reservada, confidencial o secreta.
- La información a los documentos se realiza mediante URL, direccionamiento utilizado en páginas web, de manera que las personas que copian la dirección URL de un documento pueden volver a acceder al documento sin necesidad de utilizar la aplicación de gestión documental.
- La aplicación no considera el envío de documentación interna en la Institución.
- La opción de asignación de tiempos solamente se queda registrada en la hoja de ruta pero no genera opciones de alarmas.
- La aplicación instalada actualmente almacena los documentos en un repositorio de información, no obstante la empresa que brinda el soporte en la herramienta principal no brinda soporte técnico en este software.
- No se almacena documentos generados internamente a fin de formar un expediente único de un caso.
- La herramienta solo considera envío de documentos entre las áreas existentes pero no los flujos de documentos en los diferentes procesos.
- No todos los documentos tanto internos y externos son ingresados al Gestor Documental.

- La documentación de la SCPM no cuenta con un solo repositorio digital.
- No toda la documentación que se genera en la SCPM es digitalizada.
- No toda la documentación que se genera en la SCPM es enviada a la Dirección de Secretaría General, es decir la documentación que se genera en la SCPM se encuentra dispersa en las diferentes unidades.
- La documentación relacionada con expedientes y denuncias es receptada en la Dirección de Secretaría General y se traslada físicamente desde esta unidad, pasando por varias unidades hasta llegar a su destinatario final.
- No existe un procedimiento para el tratamiento de información que se deber dar a los documentos físicos y digitales.

A continuación se realiza un levantamiento de información referente a documentación externa, documentación interna, archivo de expediente, custodia de expediente, documentación externa (pública), documentación externa (confidencial) y documentación externa (secreta).

4.1.9. Documentación externa

El tratamiento actual de la documentación externa que maneja la SCPM se describe en la **Figura 4.2**, en la misma se puede observar que el Departamento de Secretaría General tiene una gran responsabilidad al momento de manipular cualquier documento ya que es el único ente encargado de recepción formal de información que arribe a la Institución; de igual manera es el departamento encargado de canalizar de manera correcta la entrega de información.

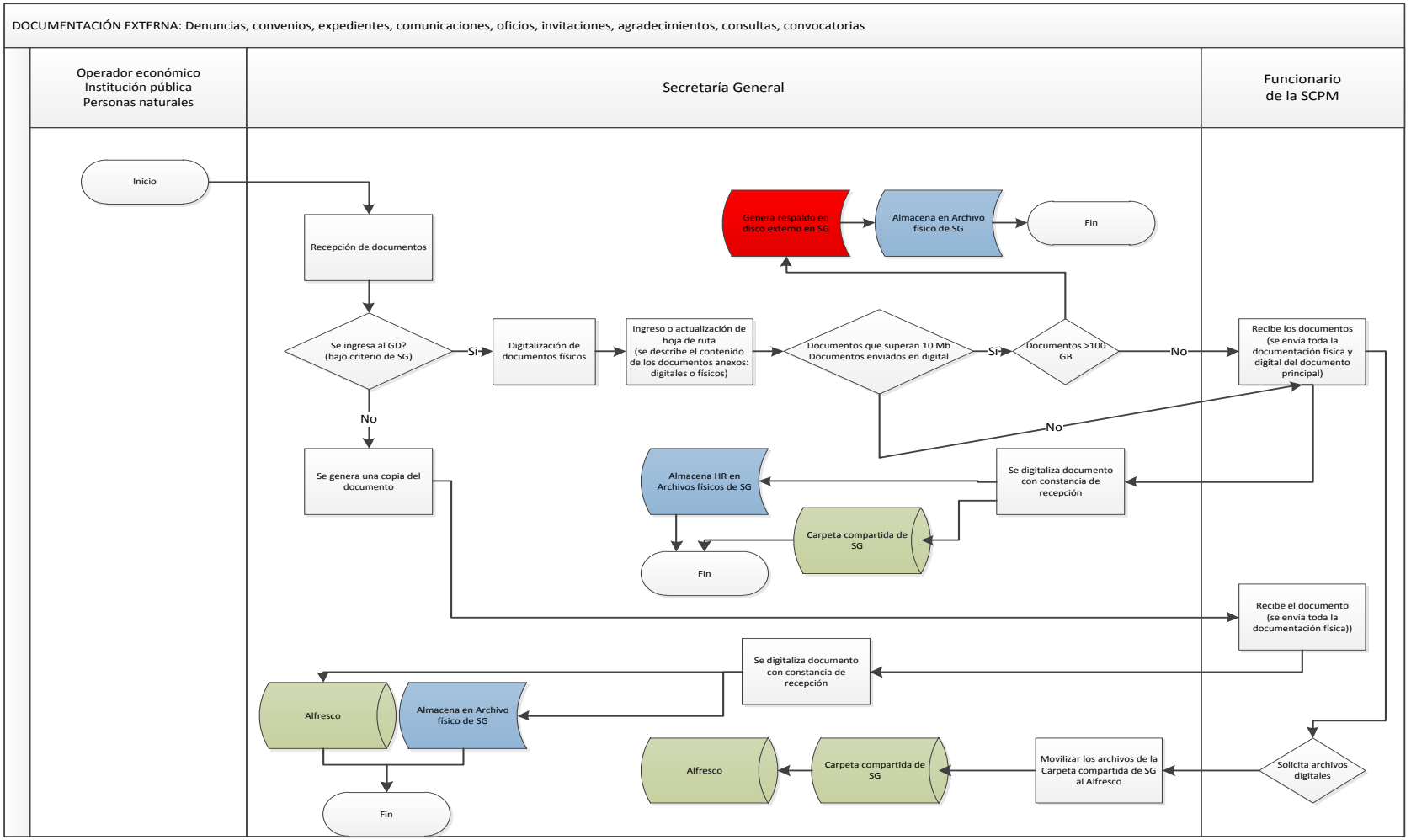

Figura 4.2 **Flujo de documentación externa de la SCPM. Elaborado por autor.**

4.1.10. Documentación interna

El tratamiento actual de la documentación interna que maneja la SCPM se describe en la **Figura 4.3**, en la misma se puede observar que el Departamento de Secretaría General tiene una gran responsabilidad al momento de manipular cualquier documento que se genere en interno por cada una de las áreas con que cuenta la Institución.

Toda la documentación que se genera en interno se encuentra canalizada a través del departamento de Secretaria General.

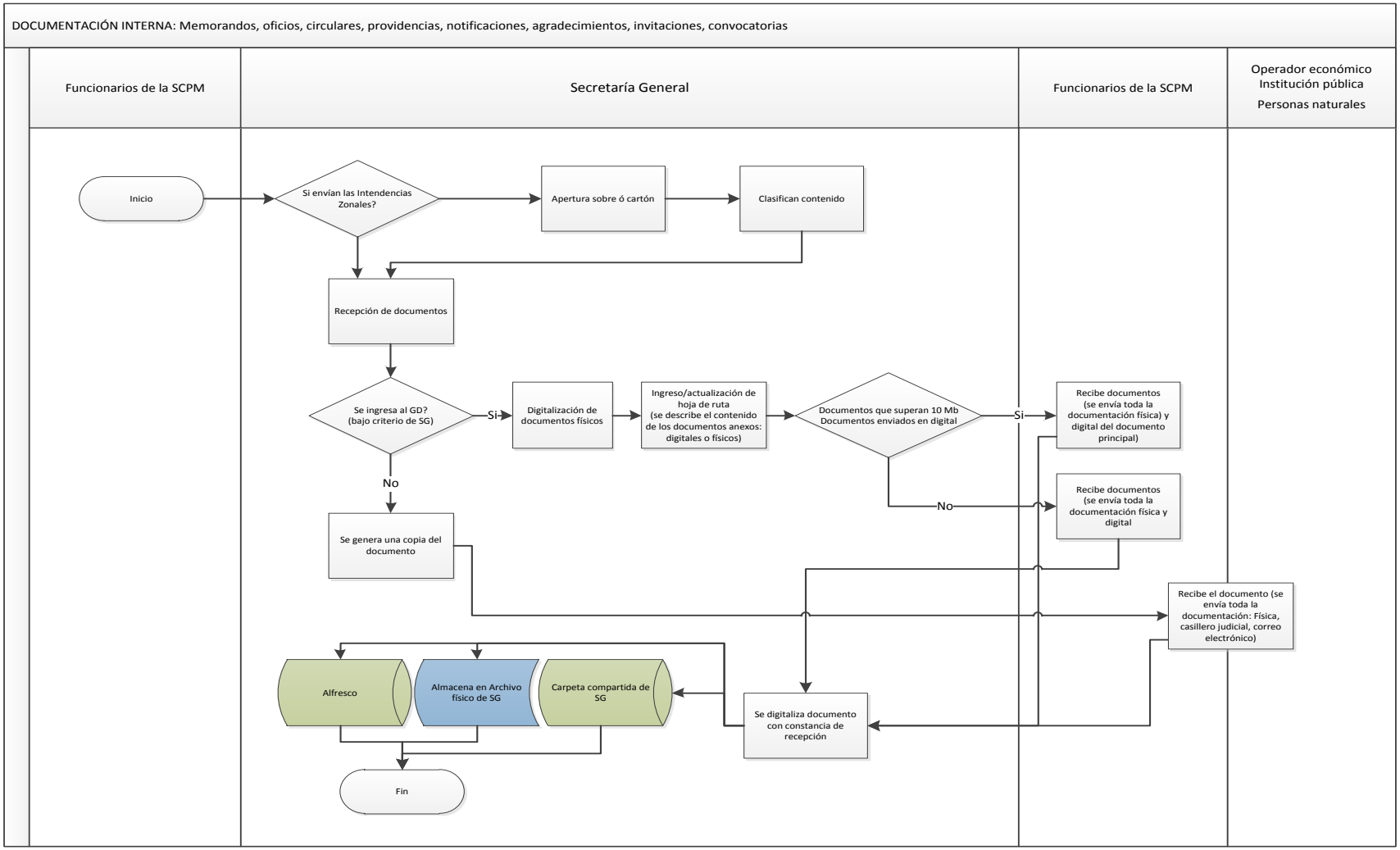

Figura 4.3 **Flujo de documentación interna de la SCPM. Elaborado por autor.**

4.1.11. Archivo de expediente

El tratamiento actual de archivo de documentación que maneja la SCPM se describe en la **Figura 4.4**, en la misma se puede observar que el Departamento de Secretaría General sigue manteniendo su participación constante ya que valida que la información sea consistente para poder archivar la misma; si la información no cumple con ésta característica es devuelta al funcionario que la generó para que rectifique y pueda ser archivada de manera correcta.

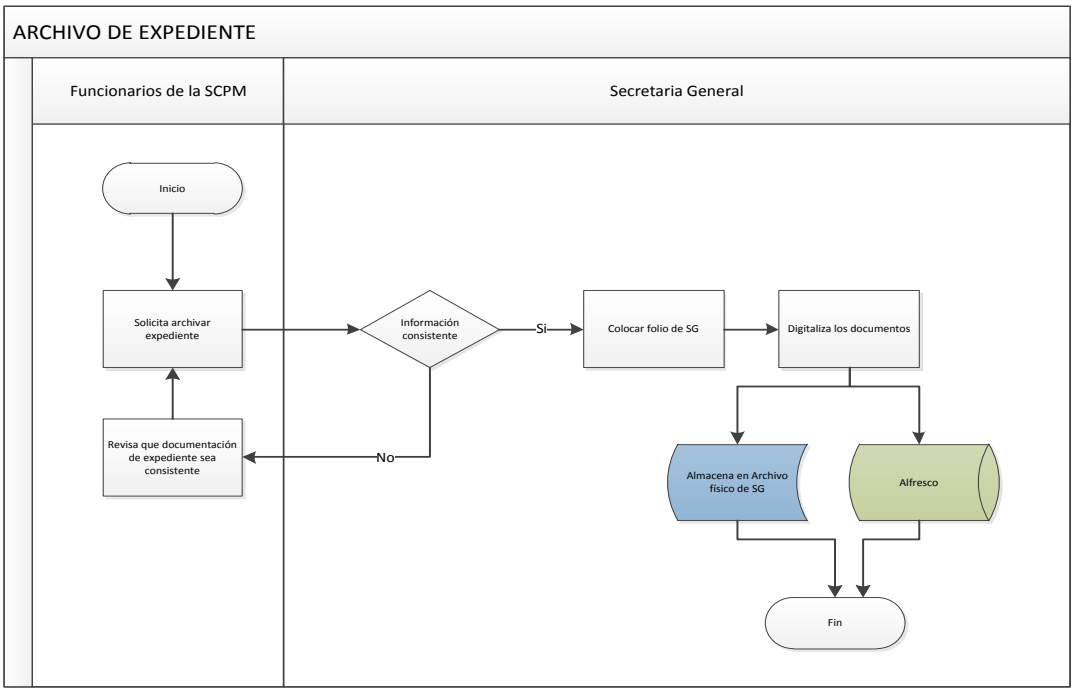

Figura 4.4 **Flujo de archivo de expediente de la SCPM. Elaborado por autor**.

4.1.12. Custodia de expediente

El tratamiento actual para custodia de expedientes que maneja la SCPM se describe en la **Figura 4.5**, en la misma se puede observar que el Departamento de Secretaría General sigue manteniendo su participación constante ya que valida que la información sea consistente para poder archivar la misma; si la

información no cumple con ésta característica es devuelta al funcionario que la generó para que rectifique y pueda ser digitalizada y archivada de manera correcta.

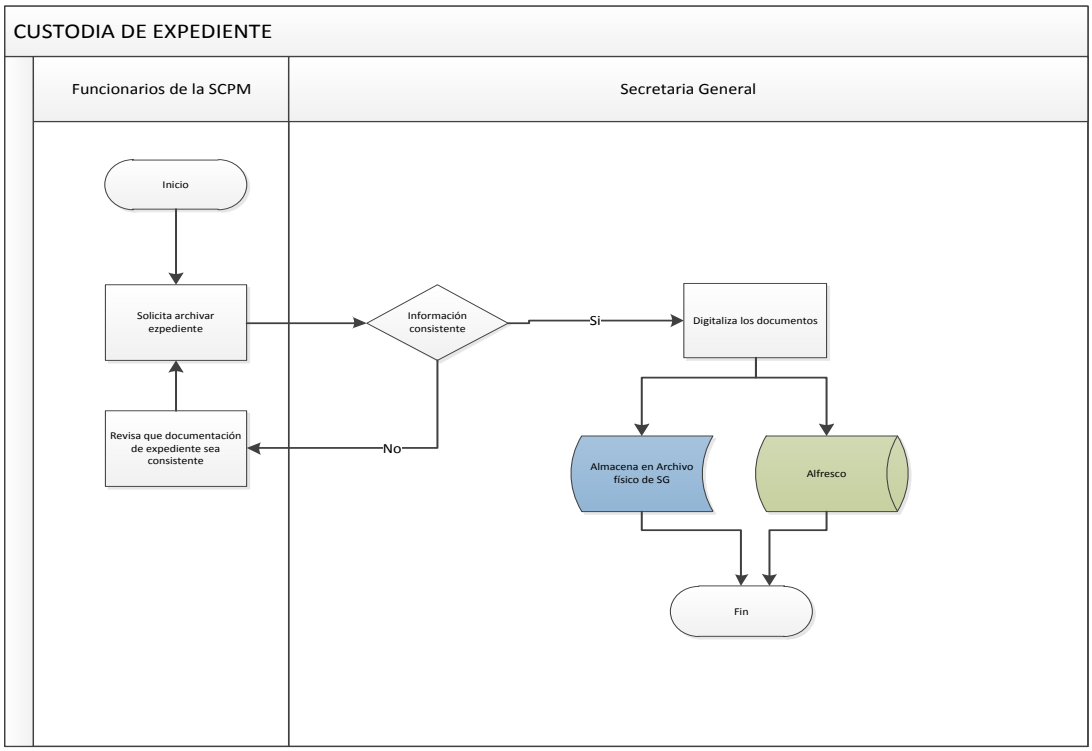

Figura 4.5 **Flujo custodia de expediente de la SCPM. Elaborado por autor.**

4.1.13. Documentación externa pública

El tratamiento actual para la documentación externa pública que maneja la SCPM se describe en la **Figura 4.6**, en la misma se puede observar que el Departamento de Secretaría General sigue manteniendo su participación constante para registro y almacenamiento de información.

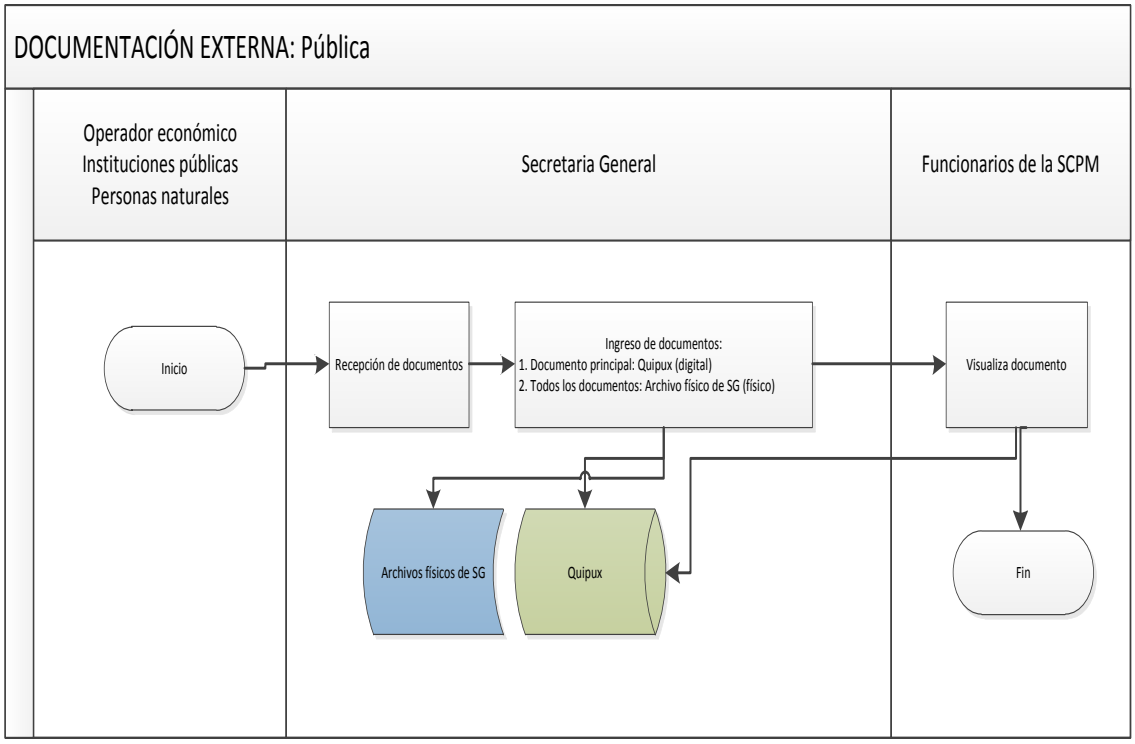

Figura 4.6 **Flujo de documentación externa pública de la SCPM. Elaborado por autor.**

4.1.14. Documentación externa confidencial

El tratamiento actual para la documentación externa confidencial que maneja la SCPM se describe en la **Figura 4.7**, en la misma se puede observar que el Departamento de Secretaría General sigue siendo un actor principal en el flujo para tratamiento de esta información, por lo que se lo debe tener muy en cuenta para el planteamiento del presente proyecto.

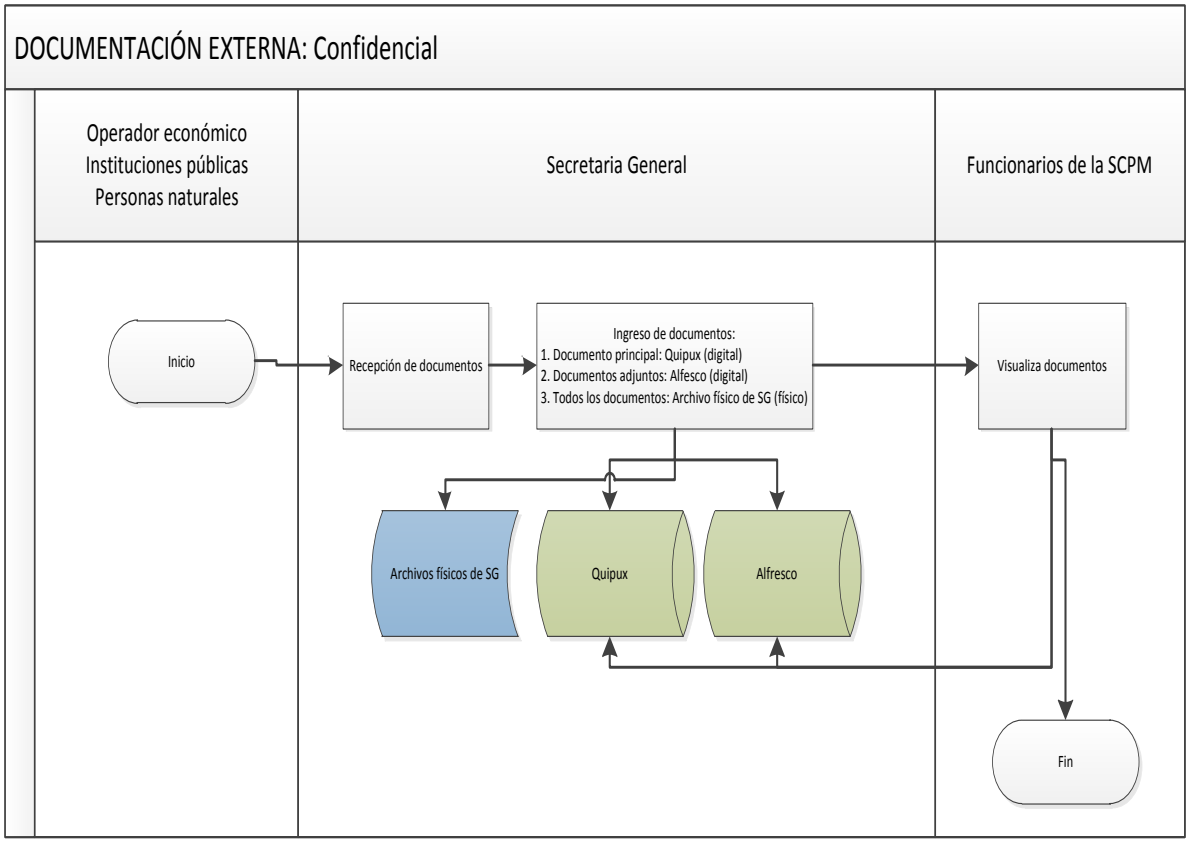

Figura 4.7 **Flujo de documentación externa confidencial de la SCPM. Elaborado por autor.**

4.1.15. Documentación externa secreta

El tratamiento actual para la documentación externa secreta que maneja la SCPM se describe en la **Figura 4.8**, en la misma se puede observar que el Departamento de Secretaría General sigue siendo un actor principal en el flujo para tratamiento de esta información, por lo que se lo debe tener muy en cuenta para el planteamiento del presente proyecto.

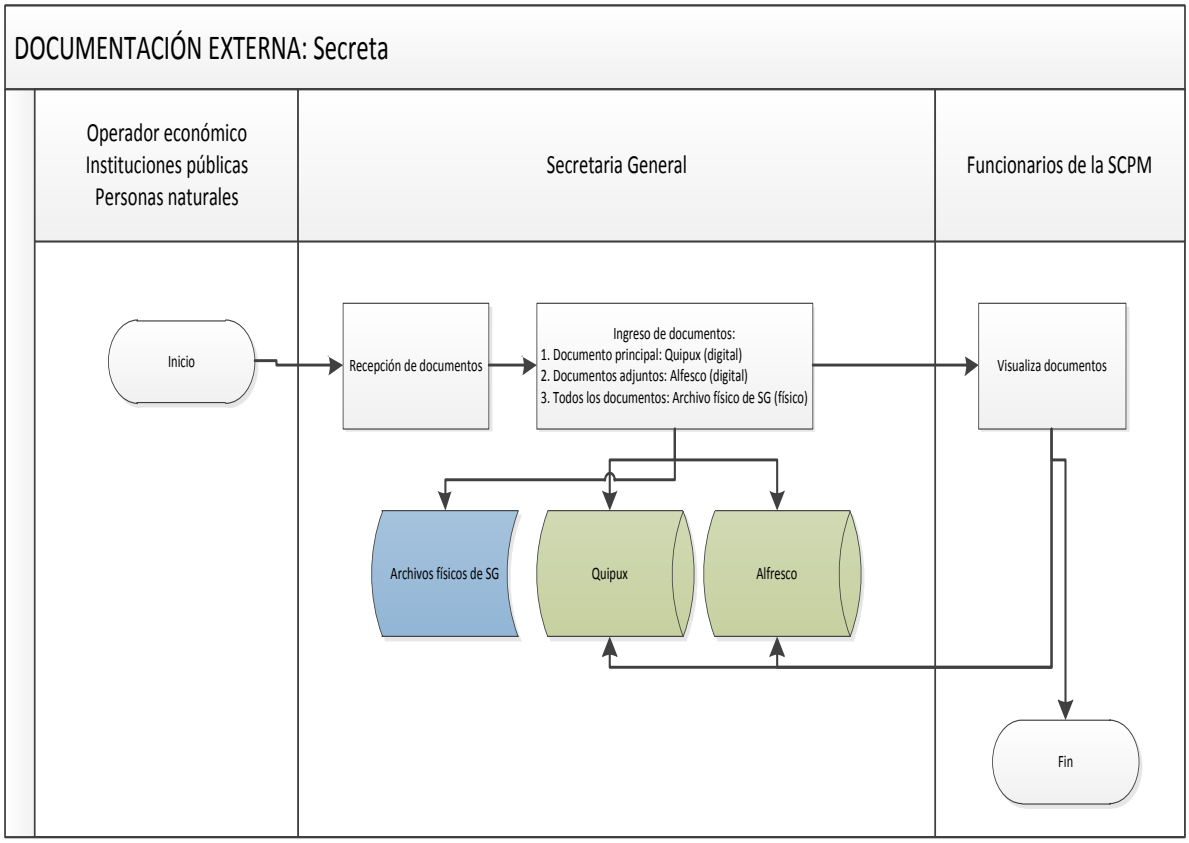

Figura 4.8 **Flujo de documentación externa secreta de la SCPM. Elaborado por autor.**

4.2. Análisis acerca del estado de infraestructura actual donde reposa la documentación actual que maneja la SCPM

La SCPM cuenta con infraestructura tecnológica recientemente adquirida, al contar con esta variable se procede a realizar un escaneo de las posibles vulnerabilidades con que pueda contar la red.

4.2.1. Planos de la oficina matriz de la SCPM

La SCPM funciona permanentemente en las oficinas ubicadas en las calles José Bosmediano y José Carbo en el sector de Bellavista – Quito (Ex fundación Guayasamín). Las oficinas son atípicas ya que las mismas fueron adaptadas para que la institución pueda trabajar de manera normal. La misma se encuentra distribuida de la siguiente manera, como se muestra en la **Figura 4.9**.

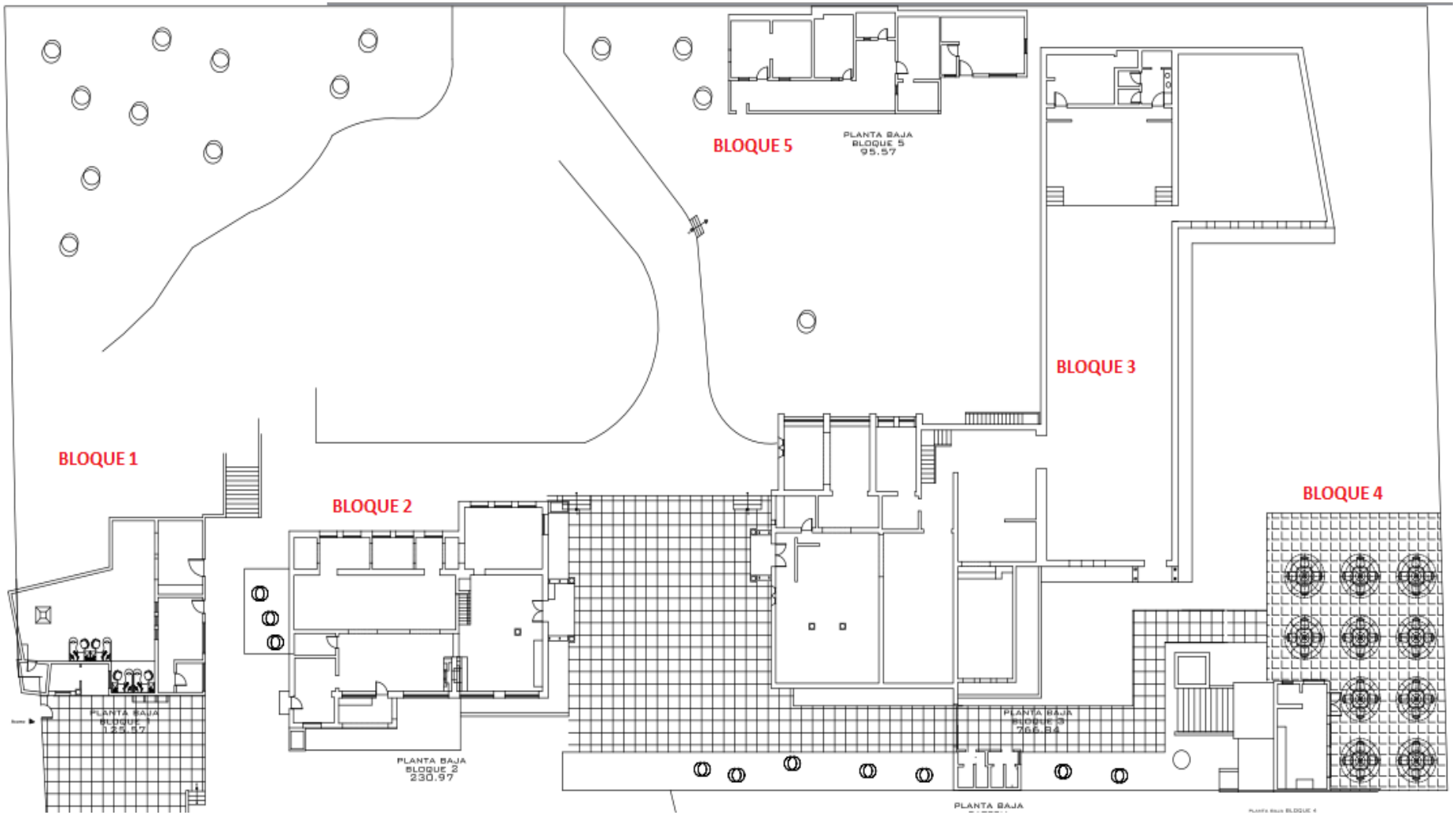

Figura 4.9 **Planos de la oficina Matriz de la SCPM. Elaborado por autor.**

4.2.2. Esquema de Infraestructura de Red oficina Matriz.-

A continuación se presenta el esquema actual con el que cuenta la SCPM en su oficina Matriz.

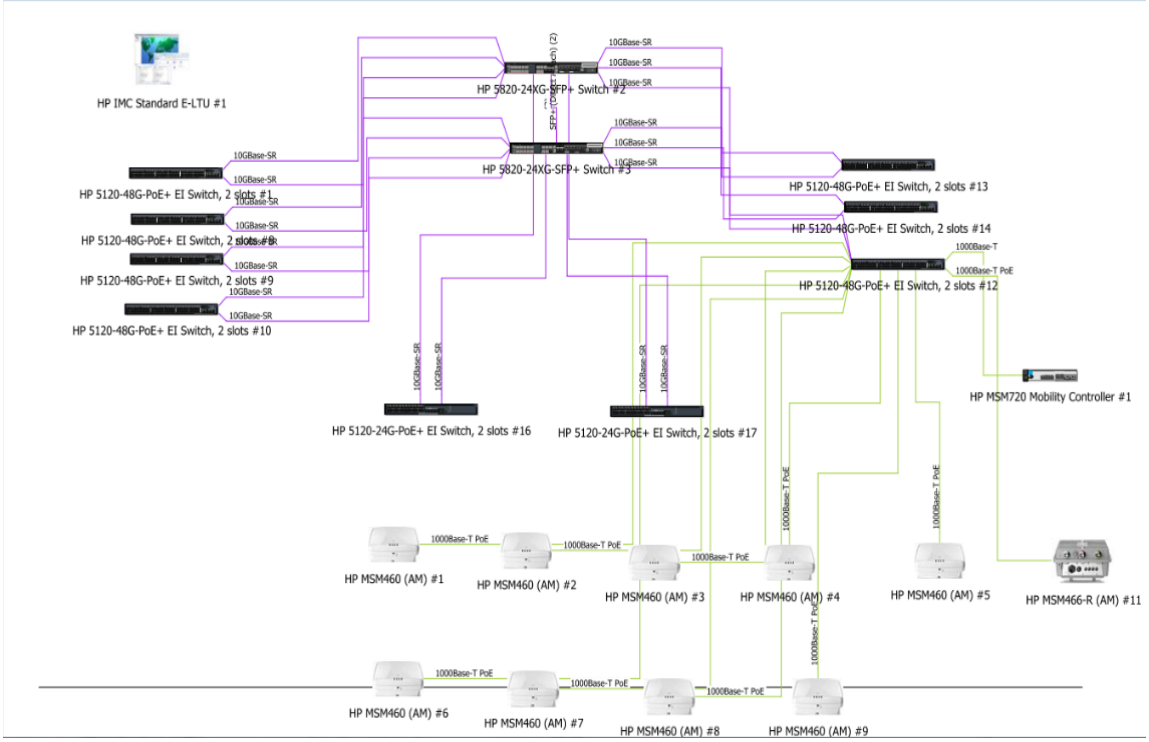

Figura 4.10 **Estructura de red SCPM Matriz. Elaborado por autor.**

Se realizó el diseño de red tomando en cuenta los conceptos de confiabilidad, escalabilidad, seguridad y convergencia, así como también las mejores prácticas de la industria y recomendaciones del fabricante de los equipos HP Networking.

El equipamiento que forma parte de la infraestructura es:

4.2.2.1. Core y Distribución.-

Formado por dos Switches HP 5820-24XG-SFP+ en configuración IRF, logrando con esto ver a los equipos como un solo equipo en él se

encuentra implementada toda la funcionalidad de capa 3, esto es: usuarios de administración, esquema de ruteo, vlans, vlans interfaces, listas de acceso, links aggregations que permiten la conectividad con los equipos de acceso a través del enlace de fibra de 10Gbps.

Los 2 puertos finales de cada uno de los switches 5820, son utilizados para realizar la configuración del IRF. La conectividad con los switches de acceso de cada bloque está dado por 2 enlaces de fibra (1 fibra principal, 1 fibra redundante) que se conectan al Core mediante 2 puertos de fibra de los switches 5820 distribuidos uno en cada unidad del IRF, logrando con esto obtener redundancia.

4.2.2.2. Acceso.-

Formado por 3 Switches HP A5120-24G-PoE + EI Switch y 7 Switches HP 5120-48G-PoE+, distribuidos en de la siguiente manera:

- Bloque 1: Dos (2) Switch HP A5120-48G-PoE + EI.
- Bloque 2: Un (1) Switch HP 5120-48G-PoE+ EI.
- Bloque 3: Dos (2) Switch HP 5120-48G-PoE+ EI.
- Bloque 3A: Un (1) Switch HP A5120-24G-PoE + EI y un (1) Switch HP 5120-48G-PoE+ EI.
- Bloque 4: Un (1) Switch HP A5120-24G-PoE + EI y un (1) Switch HP 5120-48G-PoE+ EI.
- Bloque 5: Un (1) Switch HP 5120-24G-PoE+ EI.

En los switches se encuentran configuradas vlans definidas por la Superintendencia de Control del Mercado de la siguiente manera:

Tabla 4.1 **Esquema de VLANS SCPM. Elaborado por autor.**

VLANS				
ID VLAN	**Descripción**	**Subred**	**Máscara**	**VLAN Interface**
1	Administración Equipos	10.10.1.0	255.255.255.0	10.10.1.254
2	Ruteo	192.168.1.0	255.255.255.252	192.168.1.1
3	Servidores	192.168.3.0	255.255.255.0	192.168.3.254
4	Impresoras	192.168.4.0	255.255.255.128	192.168.4.126
5	Cámaras y Biométricos	192.168.4.128	255.255.255.128	192.168.3.254
6	Intendencia General	192.168.5.0	255.255.255.192	192.168.5.62
7	Financiero	192.168.5.64	255.255.255.192	192.168.5.126
8	Canal TV	192.168.5.128	255.255.255.192	192.168.5.190
9	Auditorio	192.168.5.192	255.255.255.192	192.168.5.254
10	Despacho	192.168.6.0	255.255.255.192	192.168.6.62
11	Tecnología	192.168.6.64	255.255.255.192	192.168.6.126
12	Secretaria	192.168.6.128	255.255.255.192	192.168.6.190
13	Intendencia de Investigación	192.168.6.192	255.255.255.192	192.168.6.254
14	Comunicación	192.168.7.0	255.255.255.192	192.168.7.62
15	Transporte	192.168.7.64	255.255.255.192	192.168.7.126
16	Relaciones Internacionales	192.168.7.128	255.255.255.192	192.168.7.190
17	Comisión de Resolución	192.168.7.192	255.255.255.192	192.168.7.254
18	Jurídico	192.168.8.0	255.255.255.192	192.168.8.62
19	Wireless Invitados	192.168.9.0	255.255.255.128	192.168.9.126
20	Wireless Jerárquico Superior	192.168.9.128	255.255.255.128	192.168.9.254
21	Wireless Usuarios ASPM	192.168.10.0	255.255.255.224	192.168.10.126

4.2.3. Detalle de la herramienta Nessus.-

Para este punto se ha tomado en cuenta la herramienta de monitoreo Nessus, la cual permite cumplir con este propósito.

Es un software que sirve para realizar escaneos de vulnerabilidades trabaja con una interface Web que trabaja con un servidor http y un cliente, para realizar el análisis no se necesita instalar ningún software extra ya que este trabaja con varios pluggins, nessus es un software bastante flexible permite realizar varios tipos de escaneos como detección de host conectados a la red, puertos abiertos, análisis de aplicaciones web, análisis de malware en sistemas Windows y una análisis completo de los equipos

conectados a la red, de la misma manera se puede crear políticas para generar escaneos combinados.

4.2.4. Escaneo de Vulnerabilidades Nessus

A continuación se presenta un análisis realizado con la herramienta Nessus dentro de la Superintendencia de Control del Poder de Mercado, en las mismas se encuentran las siguientes observaciones:

La **Tabla 4.2**, muestra el resumen de las vulnerabilidades y puertos abiertos del equipo HP Switch y equipo Core de la SCPM.

Tabla 4.2 **Resumen de Vulnerabilidades equipos SCPM. (Escaneo Nessus).**

Equipo		Puerto	Vulnerabilidad	Detalle	Solución
HP Switch	Bajo	22/tcp	El equipo se encuentra configurado para permitir algoritmos MD5 o MAC 96 bits	Se muestra como vulnerabilidad por que los dos algoritmos en la actualidad se consideran débiles	Consultar al proveedor para deshabilitar la opción de MD5 y MAC de 96 bits, realizar un plan de trabajo para poder habilitar un algoritmos más robusto. El equipo soporta los siguientes algoritmos: hmac-md5 hmac-md5-96 hmac-sha1-96
	Bajo	22/tcp	El equipo está configurado para admitir el cifrado Cipher Block Chaining (CBC)	Esto podría permitir a un atacante para recuperar el mensaje de texto en claro a partir del texto cifrado.	Establecer un plan de trabajo paradeshabilitar el cifrado modo de cifrado CBC, y permitir que el CTR o el cifrado modo de cifrado GCM.

La ***Figura 4.11***, muestra el porcentaje de afectación de las vulnerabilidades encontradas detalladas anteriormente en la Tabla 4.2.

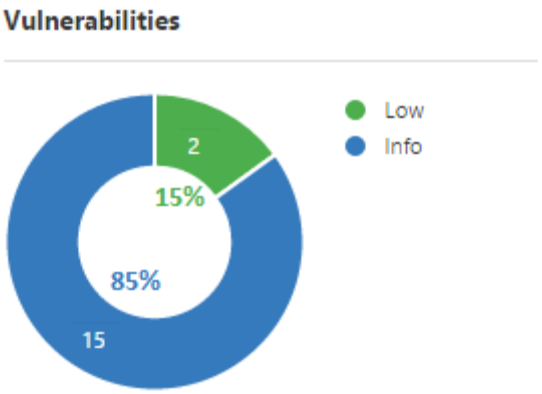

Figura 4.11 **Porcentaje de Afectación del HP Switch. (Escaneo Nessus).**

Tabla 4.3 **Vulnerabilidades cortafuegos SCPM. (Escaneo Nessus).**

Equipo		Puerto	Vulnerabilidad	Detalle	Solución
firewall.scpm.gob.ec	Medio	23/tcp	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar.	Al utilizar un canal no cifrado un atacante puede pinchar las comunicaciones con lo que podría obtener claves, información sensible y modificar el tráfico.	Desactivar el servicio Telnet y utilizar SSH.
	Bajo	2220/tcp	El equipo se encuentra configurado para permitir algoritmos MD5 o MAC 96 bits	Se muestra como vulnerabilidad por que los dos algoritmos en la actualidad se consideran débiles	Consultar al proveedor para deshabilitar la opción de MD5 y MAC de 96 bits, realizar un plan de trabajo para poder habilitar un algoritmos más robusto. El equipo soporta los

					siguientes algoritmos: hmac-md5 hmac-md5-96 hmac-sha1-96
	Bajo	2220/tcp	El equipo está configurado para admitir el cifrado Cipher Block Chaining (CBC)	Esto podría permitir a un atacante para recuperar el mensaje de texto en claro a partir del texto cifrado.	Establecer un plan de trabajo para deshabilitar el cifrado modo de cifrado CBC, y permitir que el CTR o el cifrado modo de cifrado GCM.

La **Figura 4.12**, muestra el porcentaje de afectación de las vulnerabilidades encontradas detalladas anteriormente en la **Tabla 4.3**.

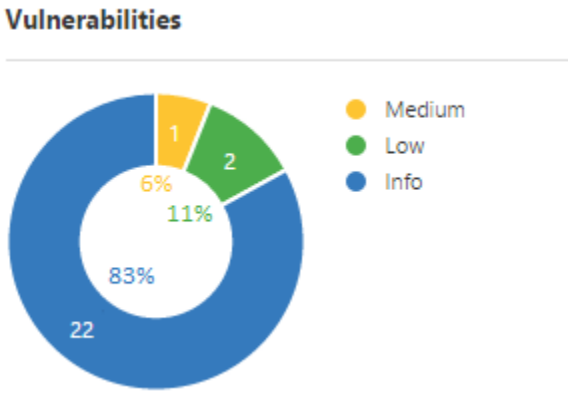

Figura 4.12 **Porcentaje de Afectación del Firewall. (Escaneo Nessus).**

Tabla 4.4 **Vulnerabilidades servidor UIO-SRVFILESERV. (Escaneo Nessus).**

Equipo		Puerto	Vulnerabilidad	Detalle	Solución
	Critica	80/tcp	El host remoto de Windows se ve afectado por una vulnerabilidad en la pila del protocolo HTTP.	La versión de Windows que se ejecuta en el host remoto se ve afectada una vulnerabilidad en la pila del protocolo HTTP (HTTP.sys)	Microsoft ha publicado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012, y 2012 R2

UIO-SRVFILESERV				debido a la inadecuada análisis sintáctico peticiones HTTP manuales. Un atacante puede aprovechar esto para ejecutar código arbitrario con privilegios del sistema.	
	Critica	5555/tcp	El host remoto se ve afectado por múltiples vulnerabilidades.	El control remoto HP Data Protector instalación se ve afectado por múltiples vulnerabilidades que podrían permitir a un atacante remoto obtener privilegios elevados, provocar una vulnerabilidad de denegación de servicio, o en el peor de los casos, ejecutar código arbitrario.	Parche la instalación según asesor del vendedor.
	Alta	2048/udp	Es posible acceder a los recursos compartidos NFS remotos sin tener privilegios de root.	Un atacante puede explotar este problema para ganar leer (y posiblemente escribir) el acceso a los archivos en el host remoto.	Configurar NFS en el host remoto para que los anfitriones sólo las personas autorizadas pueden montar las acciones remotas. El servidor

					NFS remoto debe evitar peticiones de montaje procedentes de un puerto no privilegiado.
	Media	445/tcp	Firma no es necesaria en el servidor SMB remoto.	Firma no es necesaria en el servidor SMB remoto. Esto puede permitir ataques man-in-the-middle contra el servidor SMB.	Hacer cumplir la firma de mensajes en la configuración del host.
	Media	2049/udp	El servidor permite realizar más de una acción	El servidor NFS remoto está exportando una o más acciones sin restringir el acceso (basado en el nombre de host, IP o rango de direcciones IP).	Coloque las restricciones apropiadas en todos los recursos compartidos NFS.
	Media	2049/udp	Es posible acceder a los recursos compartidos NFS en el host remoto.	Al menos uno de los recursos compartidos NFS exportados por el servidor remoto puede ser montado por el anfitrión de exploración. Un atacante podría aprovechar esto para leer archivos en el host remoto.	Configurar NFS en el host remoto de manera que sólo los hosts autorizados puedan montar sus acciones remotas.

La **Figura 4.13**, muestra el porcentaje de afectación de las vulnerabilidades encontradas en el servidor de archivos detalladas anteriormente en la **Tabla 4.4**.

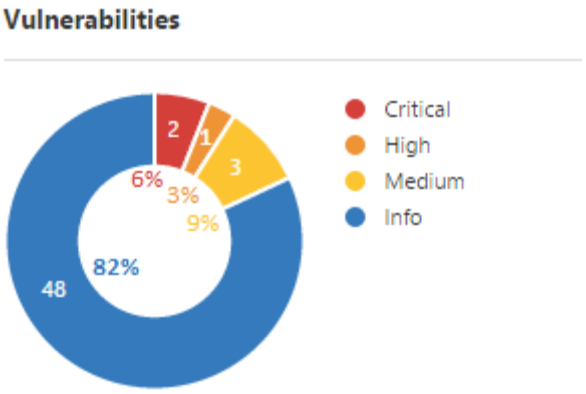

Figura 4.13 **Vulnerabilidades Servidor de archivos. (Escaneo Nessus).**

Tabla 4.5 **Vulnerabilidades WAC. (Escaneo Nessus).**

Equipo		Puerto	Vulnerabilidad	Detalle	Solución
WAC	Media	443/tcp	El certificado SSL para este servicio no se puede confiar.	Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida.	Compra o generar un certificado adecuado para este servicio.
	Media	443/tcp	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.	Compra o generar un certificado adecuado para este servicio.
	Media	443/tcp	Es posible obtener información sensible desde el host remoto con SSL / servicios	El host remoto se ve afectado por una vulnerabilidad (MitM) la divulgación de información-man-	Desactivar SSLv3. Servicios que deben soportar SSLv3 debería permitir que el

			habilitados para TLS.	in-the-middle conocido como CANICHE. Atacantes MitM puede descifrar un byte de un texto cifrado en tan sólo 256 intentos seleccionado si son capaces de forzar una aplicación víctima para enviar varias veces los mismos datos a través de nueva creación SSL	mecanismo de TLS
	Media	443/tcp	El servicio remoto encripta el tráfico mediante un protocolo con debilidades conocidas.	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes. NIST ha determinado que SSL 3.0 ya no es aceptable para las comunicaciones seguras.	Usar TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.
	Media	8082/tcp	El servicio remoto encripta el tráfico mediante un protocolo con debilidades conocidas.	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques	Usar TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

				man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los clientes. NIST ha determinado que SSL 3.0 ya no es aceptable para las comunicaciones seguras.	
	Media	8082/tcp	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.	Compra o generar un certificado adecuado para este servicio.
	Media	8082/tcp	Es posible obtener información sensible desde el host remoto con SSL / servicios habilitados para TLS.	El host remoto se ve afectado por una vulnerabilidad (MitM) la divulgación de información-man-in-the-middle conocido como CANICHE. Atacantes MitM puede descifrar un byte de un texto cifrado en tan sólo 256 intentos seleccionado si son capaces de forzar una aplicación víctima para enviar varias veces los mismos datos a	Desactivar SSLv3. Servicios que deben soportar SSLv3 debería permitir que el mecanismo de TLS

				través de nueva creación SSL	
	Media	8082/tcp	El servicio remoto es compatible con el uso del sistema de cifrado RC4.	El host remoto es compatible con el uso de RC4 en uno o más conjuntos de cifrado. El sistema de cifrado RC4 es defectuoso en su generación de una corriente pseudo-aleatoria de bytes de modo que una amplia variedad de pequeños sesgos se introduce en la corriente, disminuyendo su aleatoriedad. Si texto plano se encripta en repetidas ocasiones (por ejemplo, cookies HTTP), y un atacante es capaz de obtener muchos (es decir, decenas de millones) textos cifrados, el atacante puede ser capaz de derivar el texto en claro.	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de sistemas de cifrado RC4. Considere el uso de TLS 1.2 con suites AES-GCM sujetas a navegador y soporte de servidor web.
	Medio	8082/tcp	El servicio remoto encripta el tráfico mediante un protocolo con debilidades conocidas.	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectados por varias fallas criptográficas. Un atacante puede explotar estas fallas para realizar ataques man-in-the-middle o descifrar las comunicaciones entre el servicio afectado y los	Usar TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

				clientes.	
	Baja	22/tcp	SSH está configurado para permitir MD5 y algoritmos MAC 96 bits.	El servidor SSH está configurado para permitir ya sea MD5 o algoritmos MAC 96 bits, ambos de los cuales se consideran débiles.	Póngase en contacto con el vendedor o consulte la documentación del producto para deshabilitar MD5 y algoritmos MAC de 96 bits
	Baja	22/tcp	El servidor SSH está configurado para utilizar Cipher Block Chaining.	El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto podría permitir a un atacante para recuperar el mensaje de texto en claro a partir del texto cifrado.	Establecer un plan de trabajo paradeshabilitar el cifrado modo de cifrado CBC, y permitir que el CTR o el cifrado modo de cifrado GCM.

La **Figura 4.14**, detalla el porcentaje de afectación de las vulnerabilidades encontradas en la WAC detalladas anteriormente en la **Tabla 4.5**.

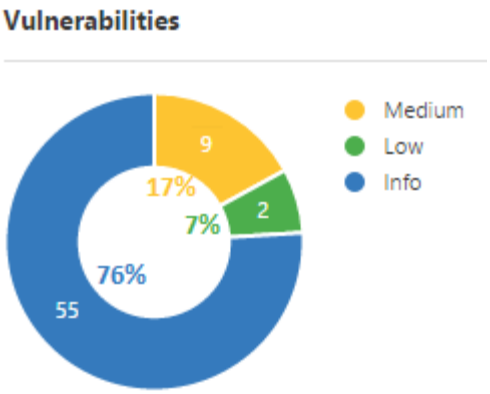

Figura 4.14 **Vulnerabilidades de la Wac. (Escaneo Nessus).**

Tabla 4.6 **Vulnerabilidades equipos zonales SCPM. (Escaneo Nessus).**

Zonales		Puerto	Vulnerabilidad	Detalle	Solución
172.16.3.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.
172.16.5.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.
172.16.6.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.

172.16.7.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.
172.16.9.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.
172.16.9.1	Medio	443/tcp	El certificado SSL para este servicio no se puede confiar.	Certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida.	Compra o generar un certificado adecuado para este servicio.
172.16.9.1	Medio	443/tcp	La cadena de certificados SSL para este servicio termina en un certificado con firma reconocida.	La cadena de certificados X.509 para este servicio no está firmado por una autoridad de certificación reconocida. Si la máquina remota es un anfitrión pública en la producción, esto anula el uso de SSL como cualquiera podría establecer un ataque man-in-the-middle	Compra o generar un certificado adecuado para este servicio.

				contra el host remoto.	
172.16.9.1	Baja	443/tcp	La cadena de certificados X.509 utilizado por este servicio contiene certificados con claves RSA de menos de 2048 bits.	Al menos uno de los certificados X.509 enviado por el host remoto tiene una clave que es más corta que 2048 bits De acuerdo a los estándares de la industria establecidos por la Autoridad de Certificación los certificados emitidos después del 1 de enero 2014 deben ser de al menos 2048 bits.	Vuelva a colocar el certificado de la cadena con la clave RSA de menos de 2048 bits de longitud con una clave más larga, y vuelva a emitir los certificados firmados por el antiguo certificado.
172.16.10.1	Medio	23/tcp	El servidor Telnet remoto transmite el tráfico sin cifrar.	El host remoto está ejecutando un servidor Telnet través de un canal sin cifrar. Uso de Telnet través de un canal no cifrado no se recomienda como logins, contraseñas, y los comandos se transfieren en texto plano.	Desactivar el servicio Telnet y utilizar SSH.

La **Figura 4.15**, muestra el porcentaje de afectación de las vulnerabilidades de los equipos a frontera de las zonales con IPs X.X.3.1, X.X.5.1, X.X.6.1, X.X10,1 como se detalla en la **Tabla 4.6**.

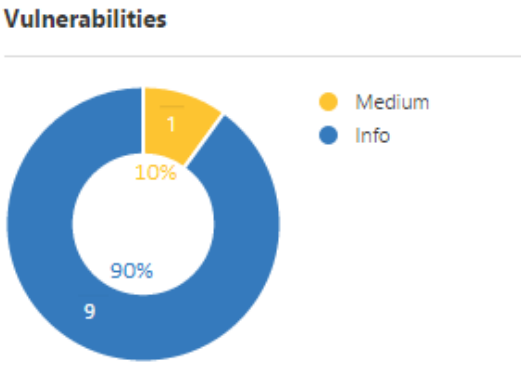

Figura 4.15 **Vulnerabilidades equipos a frontera. (Escaneo Nessus).**

La **Figura 4.16**, muestra que el equipo con IP X.X.4.1 no presenta ninguna vulnerabilidad.

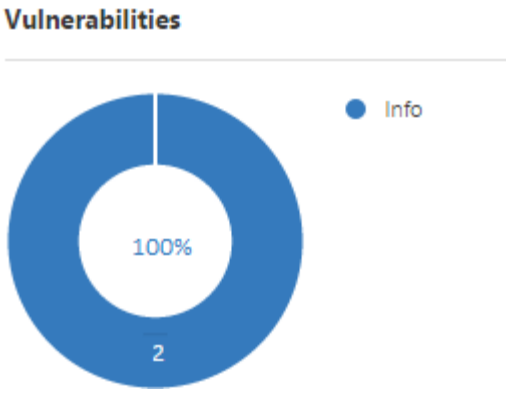

Figura 4.16 **Vulnerabilidades equipo a frontera. (Escaneo Nessus).**

La **Figura 4.17**, muestra el porcentaje de afectación de las vulnerabilidades del equipo con IP X.X.7.1 cómo se detalla en la **Tabla 4.6**.

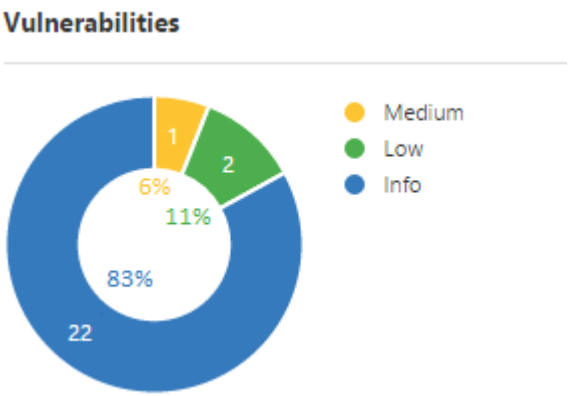

Figura 4.17 **Vulnerabilidades equipo a frontera. (Escaneo Nessus).**

La **Figura 4.18**, muestra el porcentaje de afectación de las vulnerabilidades del equipo con IP X.X.9.1 cómo se detalla en la **Tabla 4.6**.

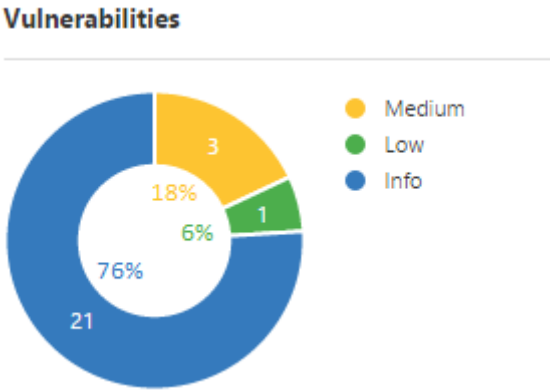

Figura 4.18 **Vulnerabilidades equipo a frontera. (Escaneo Nessus).**

4.2.5. Características técnicas de herramientas de fuga de información

- Cualquier petición de información, servicio o acción proveniente de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la institución, para realizar dicha acción; no dar seguimiento a esta política implica:

    a. Negar por completo la ejecución de la acción o servicio.

b. Informe completo dirigido a comité de seguridad, mismo será realizado por la persona o el departamento al cual le es solicitado el servicio.
c. Sanciones aplicables por autoridades de nivel superior, previamente discutidas con el comité de seguridad.

- Son usuarios de la red institucional los funcionarios, secretarias, asistentes, autoridades, y toda aquella persona, que tenga contacto directo como empleado y utilice los servicios de la red institucional de la Superintendencia de Control del Poder de Mercado.
- Se asignará una cuenta de acceso a los sistemas de red institucional, a los usuarios que lo requieran, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.
- Los funcionarios, son usuarios limitados, estos tendrán acceso únicamente a los servicios de red estrictamente necesarios y recursos compartidos requeridos, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y análisis para su implementación.
- Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la institución fuera del ámbito de empleado y siempre que tenga una vinculación con los servicios de la red institucional.
- El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

- No se proporcionará el servicio solicitado por un usuario, funcionario o departamento, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.
- La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales. Todos los funcionarios sin excepción deben cumplir con este parámetro de seguridad y acceso a la red institucional.
- El usuario es responsable exclusivo de mantener a salvo su contraseña.
- El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.
- Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.
- El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.
- El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.
- Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a los administradores del sistema u oficial de seguridad.

4.2.6. Control de acceso físico

Para el acceso físico se plantean los siguientes puntos que deben ser aplicados al modelo propuesto:

- El cableado de red, será utilizado exclusivamente por funcionarios que laboren dentro de la Superintendencia de Control del Poder de Mercado. No se habilitará la red cableada para personal ajeno a la institución.
- Los servidores, sin importar al grupo al que estos pertenezcan, deberán ser accedidos única y exclusivamente por personal que cuente con los accesos y manipulación a los mismos.
- Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el oficial de seguridad y las personas responsables por esos activos, quienes deberán poseer su debida identificación.
- Las estaciones o terminales de trabajo, con procesamientos críticos no deben contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.
- En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.
- Toda visita a las oficinas de tratamiento de datos críticos e información (dirección de tecnología, centro de datos, dirección de Secretaría General, entre otros) deberá ser registrada mediante un formulario de accesos, para posteriores análisis del mismo.

- Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.
- En la ***Figura 4.19*** se muestra un esquema de seguridad física propuesto para el tratamiento de información en la Superintendencia de Control del Poder de Mercado.

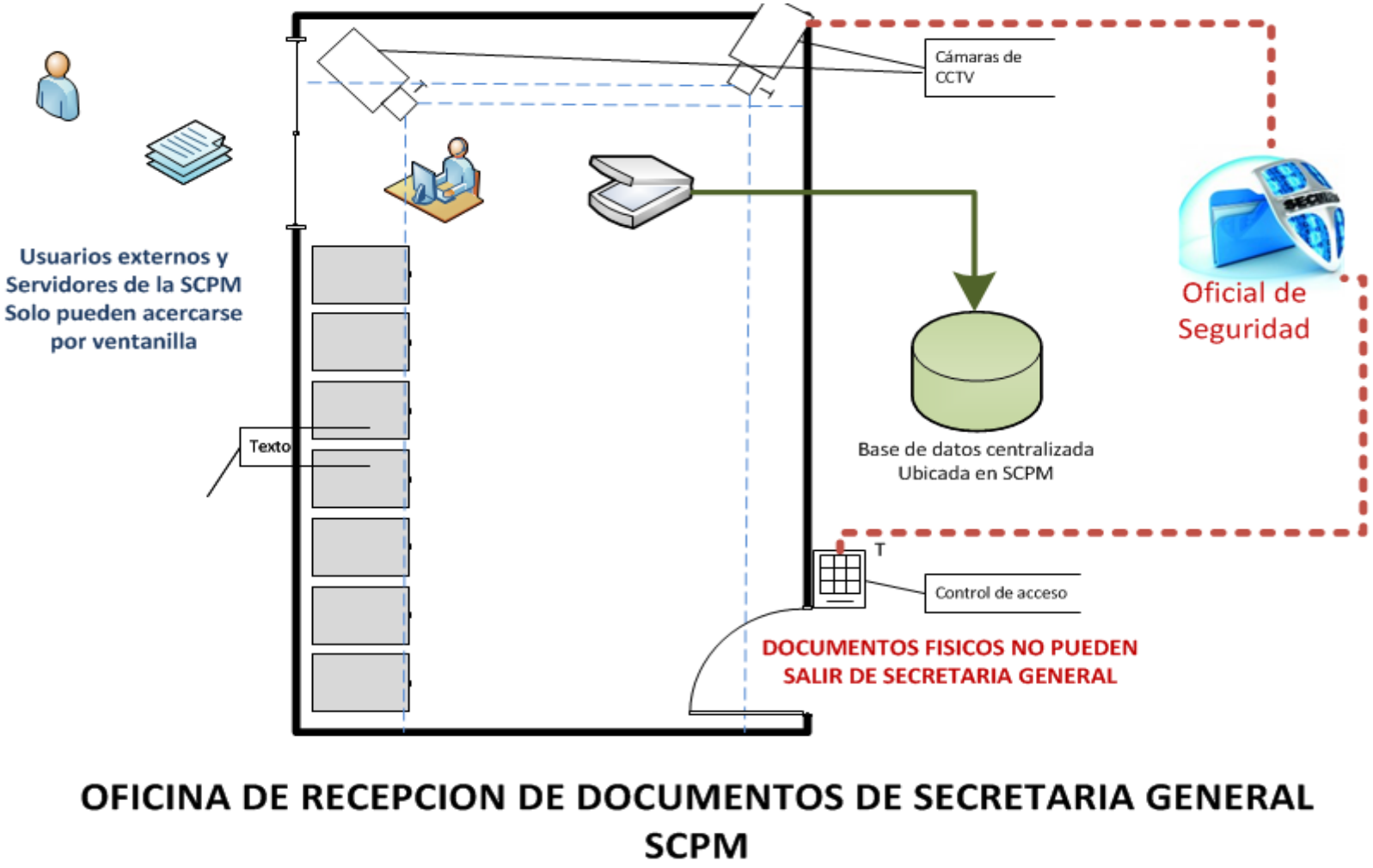

Figura 4.19 **Esquema de control de documentos SCPM. Elaborado por autor.**

Dentro del esquema propuesto en la **Figura 4.19** se pretende complementar la solución con un esquema de seguridad física para la recepción de documentos e ingreso de información al flujo informático propuesto para la Superintendencia de Control del Poder de Mercado.

El esquema contempla el ingreso único de documentos sea personal interno o externo para mantener un solo flujo a través de la Secretaria General de la Institución.

Para monitorear de manera permanente se contempla la colocación de cámaras de seguridad ubicadas estratégicamente para observar el ingreso de documentación y garantizar que la misma sea ingresada de manera adecuada.

La persona que reciba la documentación debe constar con el perfil adecuado y estar notificada (o) de manera oficial acerca de la delicadeza del trabajo y además contar con un acta que garantice la confidencialidad de sus labores, tal como se indica en el Acuerdo 166 emitido por la Secretaría Nacional de Administración Pública.

Ninguna persona ajena al departamento de Secretaría General podrá ingresar a sus dependencias, si el ingreso de alguna persona se ejecuta debe ser a través de los permisos y autorizaciones pertinentes indicando el motivo y el lugar específico a donde se dirige. El departamento debe contar con un control de acceso que avale sólo el ingreso de personal autorizado a sus dependencias.

Los archivos deben estar almacenados, custodiados y registrados de manera correcta, cumpliendo normas y estándares de documentación. Éstos documentos nunca deberán salir de la institución ni su dependencia, para ello toda la documentación será escaneada e ingresa en el repositorio único para su tratamiento adecuado, el mismo contará con el monitoreo permanente de las actividades que sucedan en el sistema de archivos.

Todas estas actividades deben ser monitoreadas por el oficial de seguridad o quién ejerza sus funciones. En el caso de existir anomalías o supuestos movimientos atípicos, éstos deben ser notificados de manera inmediata a las autoridades pertinentes para corregir las observaciones de manera oportuna.

Los equipos en donde se generarán los trabajos contarán con el concepto de Hardening para reforzar la seguridad propuesta. Dentro de este concepto se contemplarán las siguientes actividades:

- **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware en el equipos.-** Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.
- **Instalación segura del sistema operativo.-** Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (1 para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.
- **Activación y/o configuración adecuada de servicios de actualizaciones automáticas.-** Para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una institución, es adecuado instalar un servidor de actualizaciones, que deberá ser

probado en un entorno de pruebas el impacto de la instalación de actualizaciones antes de instalarlas en producción.

- **Instalación, configuración y mantención de programas de** seguridad tales como Antivirus, Antispyware, y un filtro Antispam según las necesidades del sistema.
- **Configuración de la política local del sistema**, considerando varios puntos relevantes:
    - **Política de contraseñas robusta**, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.
    - **Renombramiento y posterior deshabilitación de cuentas estándar del sistema**, como administrador e invitado.
    - **Asignación correcta de derechos de usuario**, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.
    - **Configuración de opciones de seguridad generales**, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.
    - **Restricciones de software**, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.
    - **Activación de auditorías de sistema**, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.
- **Configuración de servicios de sistema**. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si el equipo no posee

tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.

- **Configuración de los protocolos de Red.** En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.
- **Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.** En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.
- **Configuración de opciones de seguridad de los distintos programas**, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.
- **Configuración de acceso remoto**. En caso de no ser estrictamente necesario, se deshabilitará el acceso remoto. Sin embargo, cuando sea necesario tener control remoto de la máquina, se lo configurará de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.
- **Configuración adecuada de cuentas de usuario**, se trabajará con cuentas de acceso limitado y utilizando la cuenta de administrador sólo en caso necesario.

- **Cifrado de archivos o unidades según las necesidades del sistema**, considerando un almacenamiento externo para las llaves de descifrado. Se considerará la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.
- **Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema**. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

Como se pude observar todas éstas acciones serán un refuerzo necesario al modelo de seguridad propuesto para el presente proyecto.

4.3. Análisis acerca del estado de documentación actual que maneja la SCPM

En la gestión de la información, se ha detectado las siguientes observaciones:

- El programa desarrollado e implementado en la SCPM no considera los criterios de seguridad de la información definidos en la Ley Orgánica de Regulación y Control del Poder de Mercado y en el Reglamento para la Aplicación de la Ley Orgánica de Regulación y Control del Poder de Mercado.
- La información que se almacena en el programa desarrollado es independiente de la información que se encuentra en el Gestor Documental de la Institución, situación que obliga a duplicar el almacenamiento de archivos, o en su defecto que los usuarios finales tengan todos un único criterio de utilizar el programa desarrollado exclusivamente para registrar tiempos de cumplimiento y el Gestor Documental para manejo de los documentos.
- El programa desarrollado no considera todas las posibles situaciones que se pueden presentar en un caso de investigación como son: suspensión, prórroga y compromiso de cese.

- Dentro de la documentación disponible, no se ha podido encontrar la aprobación de los flujos a automatizar por parte de las intendencias involucradas en el proceso de automatización.
- El programa desarrollado no considera todas las interacciones que existen entre las Intendencias y Secretaría General durante el envío y recepción de cada uno de los documentos que forman parte de un proceso.
- El programa desarrollado no considera todos los tipos de origen de casos que pueden recibir las diferentes intendencias. Así se tiene que los siguientes tipos de casos no están considerados en el programa: a). Casos de las Intendencias de Abuso de Poder y de Prácticas Desleales originados por Oficio o Administración Pública, b). Casos para Intendencia de Control de Concentraciones de tipo Informativa, Consulta Previa y Operaciones no Notificadas.
- El sistema actual no consta con la generación de un reporte con todas las etapas de un caso y sus correspondientes fechas de cumplimiento.
- En lo referente a la arquitectura de la aplicación se ha encontrado que el diagrama entidad-relación de la base de datos tiene muchas relaciones entre sus tablas lo que dificulta la obtención de reportes adecuados.

4.4. Modelo para la implementación de documentación para la SCPM

En base al modelo planteado en el capítulo tres de este proyecto nos enfocaremos en la implementación del mismo para corregir los procesos actuales con que cuenta la Superintendencia de Control del Poder de Mercado.

Cabe recalcar que luego del análisis inicial se tomará como referencia la información que se reciba y genere en los procesos agregadores de valor, ya que en los

mismos es donde se encuentra información sensible que debe ser protegida de manera eficiente.

El modelo plantea la aceptación de normas y políticas con alcance corporativo y por procesos, siendo el primer paso tener la aceptación de las normas y procedimientos por parte de las autoridades de la Institución.

Obtener el compromiso de las autoridades como respaldo a la seguridad de información es imperativo para el éxito del modelo planteado. Sin este compromiso, las actividades relacionadas con la seguridad de información muy probablemente fallarán. Cualquier iniciativa que afecte a todo el personal de una institución no puede tener éxito sin el soporte y respaldo de las autoridades.

Es primordial que las autoridades vean a la seguridad de información como un tema muy serio para que de esta manera se puedan brindar los recursos apropiados. Las autoridades son quienes deben aprobar la estrategia de seguridad planteada. Para ello, el oficial de seguridad debe capacitar a las autoridades en temas de alto nivel relacionados a la seguridad de información. Con esto los funcionarios capacitados estarán en una mejor posición para apoyar las iniciativas de seguridad de información planteadas para la institución.

4.5. Adopción de buenas prácticas de seguridad de la información

Para el manejo de información y control de documentos se ha considerado puntos relevantes que se enfocan en el acuerdo 166 emitido por la Secretaria Nacional de Administración Pública y la norma ISO / IEC 27002.

Dentro de las recomendaciones se destacan los siguientes puntos:

- Contar con un área de seguridad para el tratamiento de información.
- Contar con un esquema apropiado para clasificación de la información

- Actores y responsables sobre el manejo de información
- Control de acceso a la información.
- Validar los riesgos en la información
- Contar con políticas de operación
    - Sobre la administración de la información
    - Sobre el control de acceso a los sistemas
    - Sobre el recurso humano que labora en la institución y para la institución.
    - Sobre el manejo de información confidencial
    - Sobre la aplicación de controles

4.5.1. Área de seguridad para el tratamiento de información

En el artículo 2.1 del Esquema Gubernamental de Seguridad de la Información (EGSI), se indica que la máxima autoridad de la Institución dispondrá la conformación del Comité de Gestión de la Seguridad, el mismo que involucrará la participación y cooperación de los cargos directivos de la Institución.

La Superintendencia de control del Poder de Mercado deberá monitorear a través del Comité de Gestión de la Seguridad, todos los eventos que tengan que ver con la seguridad de la información institucional. Dentro de sus funciones y responsabilidades se encuentran las siguientes:

- Definir y comunicar la estrategia de seguridad de la información alineada con la estrategia institucional.
- Controlar el cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información.

- Formular y mantener el plan de contingencia de seguridad que garantice la disponibilidad, confidencialidad e integridad de la información.
- Evaluar los riesgos de seguridad de la información y proponer acciones a incluirse en el Plan de Seguridad de la Información.
- Gestionar los accesos a los servicios tecnológicos institucionales.
- Participar en la implementación del plan de seguridad de la información.
- Monitorear e informar acerca del cumplimiento y aplicación de los procedimientos y estándares definidos para la seguridad de la información.

Ésta área deberá presentar informes periódicos o puntuales (en caso de requerirlos), donde se expongan todas observaciones encontradas para poder tomar acciones oportunas y adecuadas.

4.5.2. Actores y responsabilidades

Los actores que intervienen en la ejecución de esta metodología son de nivel corporativo y procesos, es decir debe existir personal con capacidad de decisión y personal operativo. Sus funciones deben estar claramente definidas dentro de la institución para poder brindar el apoyo adecuado al modelo planteado.

En el caso de la Superintendencia de Control del Poder de Mercado se han definido los siguientes roles:

- **Autoridades.-** encargados de la aprobación del plan de seguridad de la información propuesto.
- **Oficial de Seguridad.-** encargado de ejecutar y velar que el modelo de seguridad planteado sea ejecutado de manera permanente.

- **Tecnología.-** encargado de brindar apoyo tecnológico alineado con el modelo de seguridad planteado.
- **Funcionario.-** encargado de trabajar de manera adecuada con los lineamientos y políticas expuestas en el presente modelo.

4.5.3. Controles de acceso

En lo referente a controles de acceso se debe enfocar el acceso a través de accesos lógicos, accesos físicos y accesos ligados al personal que labora en la institución.

4.5.3.1. Control de accesos lógico

Para el flujo de información a ser manejada en el presente modelo se considera el acompañamiento de una herramienta que permita monitorear eventos relacionados con la fuga de información, considerando el esquema que se presenta en la **Figura 4.20**.

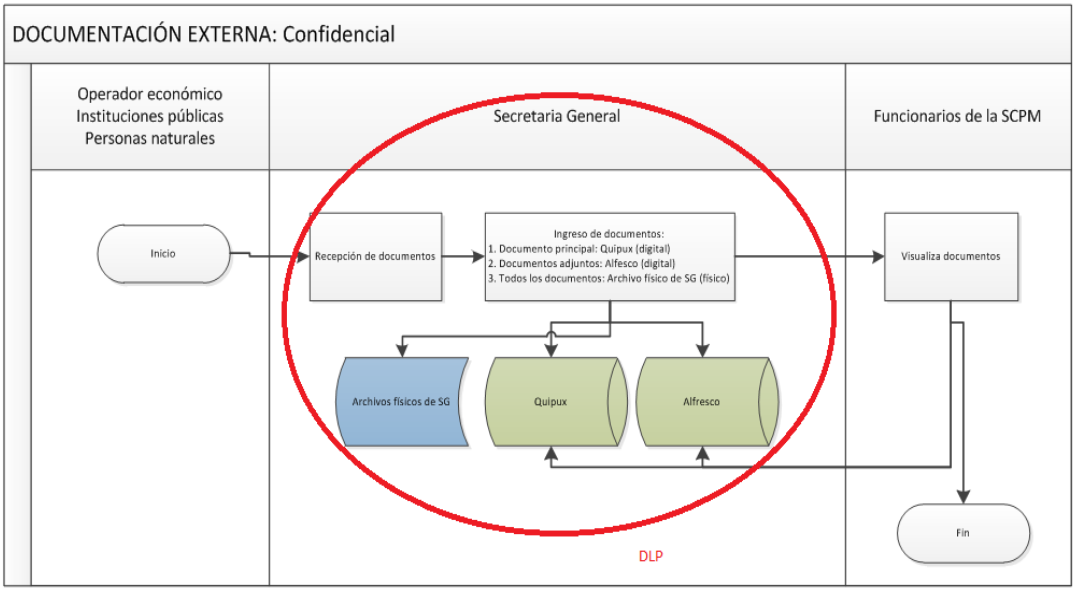

Figura 4.20 **Flujo de documentación externa con seguridad. Elaborado por autor.**

El acceso lógico debe ser monitoreado por herramienta de prevención de fuga de información como se muestra en la **Figura 4.20**. Al contar con este esquema todos los eventos que se generen en el sector de Secretaría General de la SCPM serán controlados y monitoreados directamente por el oficial de seguridad designado por la institución.

La solución de prevención de fuga de información deberá contar con las siguientes características:

- La solución debe ser totalmente compatible con la plataforma tecnológica con que actualmente cuenta la Superintendencia de Control del Poder de Mercado, garantizando operatividad, estabilidad y funcionalidad del sistema.
- Debe permitir la clasificación de la información en los niveles que la Superintendencia de Control del Poder de Mercado lo requiera, la misma deberá incluir la opción de registrar y reportar los accesos a los documentos clasificados.
- Integración con usuarios y grupos que se encuentren en el Directorio Activo de la SCPM.
- Debe permitir la creación de reglas sobre documentos etiquetados y clasificados como por ejemplo:
    - Regla que impida “copiar/pegar” a un bloc de notas.
    - Regla que bloquee el envío de documentos por correo electrónico por parte de un usuario regular.
    - Reglas para que un usuario con un nivel de usuario administrador de la carpeta confidencial pueda mover la información a la carpeta pública.

    - Reglas para restringir la impresión de documentos por usuarios no autorizados.

- Visualización de la política aplicada sobre un documento confidencial, de acuerdo con los perfiles de usuario definidos en Directorio Activo de la SCPM.
- Verificación que tanto los intentos negados de copiar o enviar información clasificada, así como el movimiento a una carpeta pública estén registrados en el log de auditoria de la herramienta.
- Se deberá visualizar un reporte, tipo log, de pistas de auditoría de las actividades realizadas sobre los documentos clasificados.

Las funcionalidades mínimas que debe tener la solución propuesta deben ser:

- Módulo de clasificación y control de seguridad de la información de punto final (*DLP*[26] *de Endpoint*).
- Control de dispositivos removibles.
- Encripción de medios.
- Encripción de directorios y archivos.
- Gestión centralizada de la política de prevención de pérdida de datos.
- Implementación de niveles de clasificación de la información.
- Clasificar y controlar el acceso a los documentos digitalizados.

[26] DLP – Data Loss Prevention.- Herramienta para prevención de fuga de información.

- Permitir la creación de tantas etiquetas como sea necesario para la adecuada clasificación de la información Institucional.
- Incluir un sistema de monitoreo que permita contar con datos históricos de acceso a documentos.
- La solución debe soportar al menos archivos con extensiones privativas: doc, docx, xls, xlsx, ppt, pptx y mpp; así como de tipo libre odt, ods, odp, odm, pdf, xml.

4.5.4. Clasificación de la información e identificación de activos

La clasificación de la información, según recomendación del artículo 3.1 del EGSI[27], es un aspecto fundamental, ya que de este punto se pueden derivar varias acciones que se deben tomar para protección de la información.

En base a la normativa tomada como lineamiento de este proyecto se realiza el siguiente análisis general de la documentación con que cuenta la Superintendencia de Control del Poder de Mercado para que esta sea protegida de manera adecuada.

Al manejar varios tipos de documentación y comunicación con usuarios internos y externos se deben considerar los siguientes puntos:

- La comunicación escrita y generada al interior de la Superintendencia de Control del Poder de Mercado debe ser canalizada de manera directa a través de la Dirección de Secretaria General, para mantener un registro de los responsables de las diferentes áreas.

[27] EGSI. Esquema Gubernamental de Seguridad de la Información. Recuperado de: http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf

- Si se requiere algún tipo de comunicación con entidades externas, las mismas deben ser canalizadas por la Dirección de Secretaria General de la Superintendencia de Control del Poder de Mercado.
- La comunicación escrita directa entre las diferentes unidades de la Superintendencia de Control del Poder de Mercado y el mundo exterior está totalmente prohibida.

En la **Figura 4.21** se muestra el flujo de los puntos expuestos:

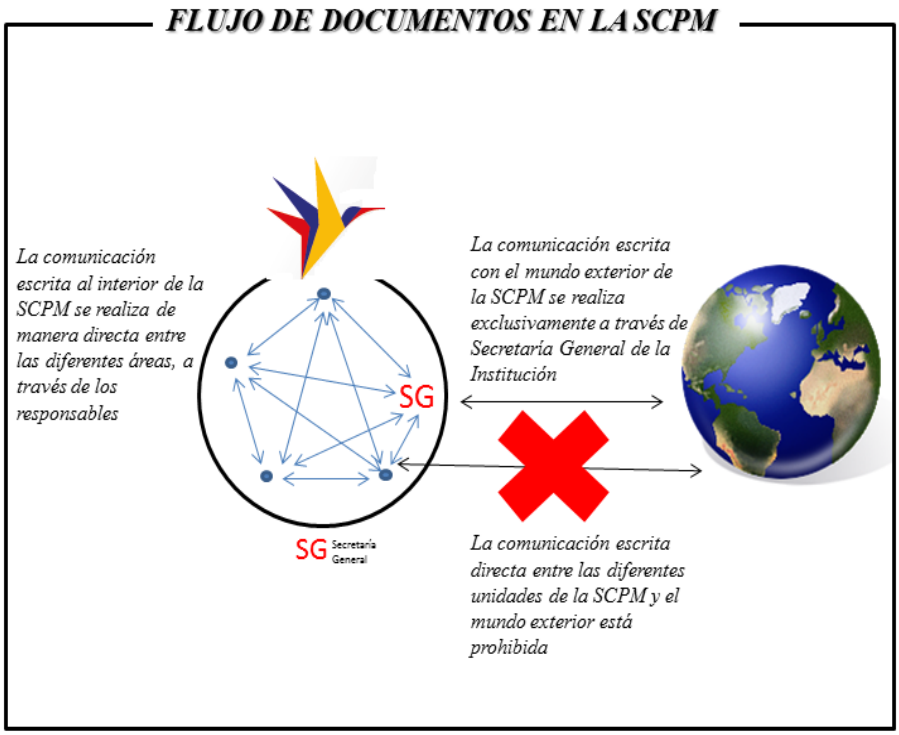

Figura 4.21 **Manejo de documentos en la SCPM. Elaborado por autor.**

- Para la comunicación interna se debe considerar el tráfico entre personal directivo y la Secretaría General de la Superintendencia de Control del Poder de Mercado como se muestra en la **Figura 4.22**.

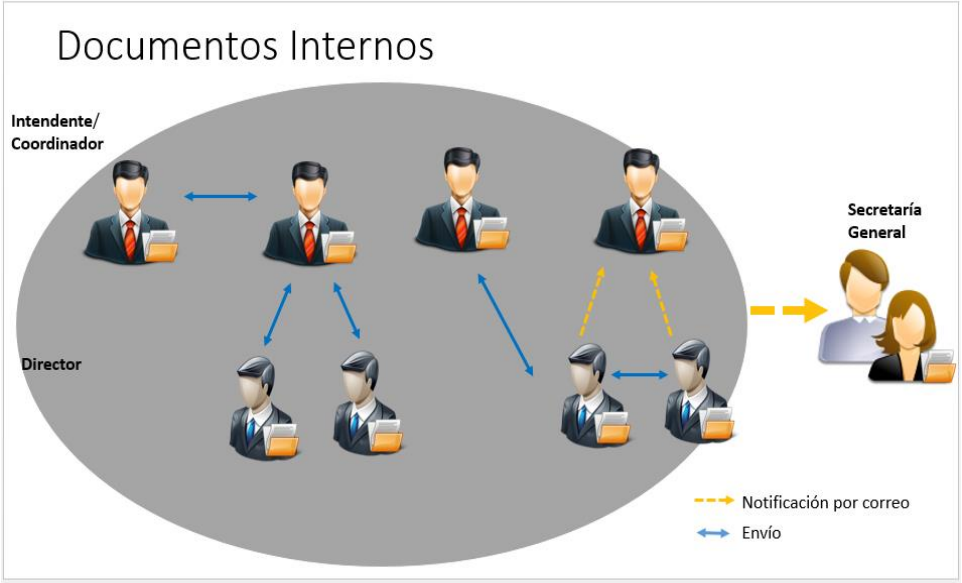

Figura 4.22 **Manejo de documentos internos en la SCPM. Elaborado por autor.**

- Para la comunicación externa se debe considerar que personal de la Superintendencia no debe por ningún motivo tener relación directa con los trámites expuestos, esto quiere decir que todo flujo debe ser canalizado por la Secretaría General de la Superintendencia de Control del Poder de Mercado como se muestra en la **Figura 4.23**:

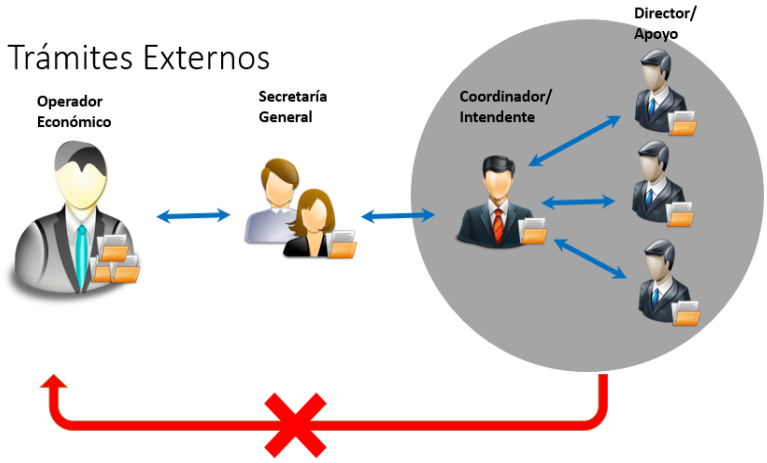

Figura 4.23 **Manejo de trámites externos en la SCPM. Elaborado por autor.**

Para el levantamiento de información se toman como referencia los siguientes puntos importantes que deben ser tomados en cuenta:

- **Tipo de activo.-** indica el tipo de información con que cuenta la institución.
- **Detalle de activo.-** indica el tipo de documento con que cuenta la institución.
- **Dueño del dato.-** indica quién es dueño y del dato que se encuentra procesado.
- **Custodio funcional.-** indica que área es responsable del activo.
- **Custodio técnico.-** indica que funcionario técnico es responsable del activo.
- **Ubicación física.-** Especifica la ubicación física del activo de información por ejemplo: archivadores, archivos de áreas, centro de cómputo, oficinas, entre otros.
- **Ubicación electrónica.-** Especifica la ubicación de los activos de información digitales que tienen ubicación electrónica por ejemplo: servidores, intranet, direcciones IP, equipos de trabajo, entre otros.

Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información dentro de la Superintendencia de Control del Poder de Mercado:

a. Pública
b. Interna
c. Confidencial
d. Secreta

Los activos de información de mayor importancia para la institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

Para el efecto de este proyecto nos centraremos en la información que se genera en los procesos agregadores de valor, ya que en los mismos es donde se tramita información sensible para la institución.

4.5.4.1. Clasificación y control de información

Para proteger activos de información primero se debe elaborar un inventario de todos los activos de información dentro de la organización para así clasificarlos por grado de importancia, y en función a ello asignar acciones de protección a los mismos. Con lo expuesto:

- Cada departamento, tendrá un responsable para mantener en custodia toda la información de mayor importancia para la institución.
- La persona o responsable de cada unidad, velará por la salvaguarda de la información, sea esta impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o hablada en conversaciones
- Los administradores de los sistemas son los responsables de la seguridad de la información almacenada en esos recursos.

4.5.4.2. Niveles de clasificación.

Los niveles de clasificación nos ayudarán a identificar la sensibilidad de la información.

- **Pública:** La información pública es la información que ha sido declarada de conocimiento público de acuerdo a alguna norma

jurídica o por parte de la persona o grupo de personas del área con autoridad para hacerlo. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que esto implique daños a terceros ni a las actividades y procesos de la Institución.

- **Interna:** Es toda información consignada en el inventario de activos de información que es utilizada por el personal de la Institución para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma leve a terceros o a los sistemas y/o procesos de la Institución.
- **Confidencial:** Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la institución.
- **Secreta:** Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización especial de la entidad. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas de la Institución.

Con la definición de los parámetros se realiza el levantamiento de información que se muestra en la **Tabla 4.7**:

Tabla 4.7 **Identificación de activos de información. Elaborado por autor.**

SCPM

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Departamento	Superintendencia de Control del Poder de Mercado
Proceso:	Superintendencia de Control del Poder de Mercado
Subproceso:	Superintendencia de Control del Poder de Mercado

Tipo Activo	Detalle de Activos	Dueño de Dato	Custodio Funcional	Custodio Técnico	Ubicación Física	Ubicación Electrónica
Información Impresa						
Expediente	Expediente para análisis de casos	SCPM	Intendencia de Prácticas desleales	Funcionario designado para revisión del expediente	Oficina de la SCPM	C:\Mis Documentos\SCPM
Información electrónica						
Avance de información de casos	Estudio de casos	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Servidor SRV-BDD-ORA	Instancia ORAPROD01 Tabla Prod01
Documentación de materia	Información referente al caso	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Equipo funcionario IPD-L-NOMBREFUN	C:\Mis Documentos\SCPM
Escaneado de expedientes	Información electrónica del caso	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Servidor SRV-FILE-SERVER	Directorio d:\datos\Expedientes

Cronograma de ejecución de casos	Detalle de fechas de ejecución de casos	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Servidor SRV-FILE-SERVER	Directorio d:\datos\Cronograma
Resolución de caso	Información de resolución de caso	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Servidor SRV-FILE-SERVER	Directorio d:\datos\Resolución
Información en Aplicativos de negocio						
SISTEMA DTS	Gestión de expedientes	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	Servidor SRV-APP-PROD
Base de Datos	Almacena información de la institución	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	Servidor SRV-BDD-ORA
Servidor de Archivos	Almacena variedad de información	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	Servidor SRV-FS
Software donde se almacena información						
Base de Datos Oracle	Base de datos, repositorio de información	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	Servidor SRV-BDD-ORA
Servicio de directorio activo	Servicio de directorio permite autenticación y autorización	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	SRV-AD
Comunicaciones para traslado de información						
Switch de core	conecta servidores con sección de acceso	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	
Switch de acceso	conecta usuarios con servidores y aplicativos	I SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	Oficina Administrativa	

Hardware que contiene información						
Servidor SRV-APP-PROD	Servidor de App de Producción	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	
Servidor SRV-BDD-ORA	Servidor de Base de datos	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	
Servidor SRV-FS	Servidor de Archivos	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	
Servidor SRV-AD	Servidor de Dominio	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	DataCenter	
Personas que tienen acceso a la información						
Intendente	Oficina IPD	SCPM	Intendencia de Prácticas desleales	Funcionario designado para revisión del expediente	Oficina IPD	
Instalaciones donde reposa información						
SCPM Bellavista	Oficina IPD	SCPM	Intendencia de Prácticas desleales	Funcionario designado para revisión del expediente	José Bosmediano y José Carbo	
Datacenter	Departamento de Tecnología	SCPM	Intendencia de Prácticas desleales	Departamento de Tecnología	José Bosmediano y José Carbo	

Una vez identificado los activos de información se procede a clasificarlos de la siguiente manera como se muestra en la ***Tabla 4.8***:

Tabla 4.8 **Clasificación de la información. Elaborado por autor.**

Superintendencia de Control del Poder de Mercado

CLASIFICACIÓN DE LA INFORMACIÓN

Activo	Detalle de Activos	Publica	Interna	Confidencial	Secreta
Expediente	Expediente para análisis de casos de prácticas desleales				X
Expediente con avance de información de casos	Análisis de estudio de casos			X	
Documentación de materia de casos	Información referente al caso			X	
Cronograma de ejecución de casos	Detalle de fechas de ejecución de casos		X		
Escaneado de expedientes	Información electrónica del caso		X		
Resolución del caso	Información de resolución de caso	X			

4.6. Evaluación de riesgos

Una vez que hayamos identificado los activos y clasificada la información esta debe ser evaluada para para ver qué tan crítica es al momento de sufrir impacto sobre ella.

4.6.1. Criterios de evaluación del riesgo

Es muy importante definir los criterios para la evaluación del riesgo, con el fin de determinar el riesgo en la seguridad de la información de la organización. Para tal efecto, se tendrán en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información del negocio
- La criticidad de los activos de información involucrados
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

Estos criterios de evaluación del riesgo se utilizarán para especificar las prioridades para el tratamiento del riesgo

4.6.2. Criterios de Impacto

Se desarrollarán criterios de impacto del riesgo y se especificarán en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando aspectos tales como:

- El nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (partes internas o terceras partes)
- Daños para la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Para el caso de estudio se realiza el levantamiento de información con la siguiente información:

- **Activos.-** indica el activo que se encuentra enfocado en su protección.
- **Amenazas.-** posible amenaza que puede ocasionar la pérdida del activo.
- **Vulnerabilidades.-** debilidades internas con que cuenta la institución.
- **Probabilidad de explotación de vulnerabilidad.-** probabilidad de materializarse la vulnerabilidad expuesta. En este caso se manejan la siguiente ponderación:

Tabla 4.9 **Ponderación de riesgos. Elaborado por autor.**

ALTO	En el corto plazo desmoviliza o desarticula a la organización.	3
MEDIO	Provoca la desarticulación de un componente del Área o de la de la Organización. Si no se atiende a tiempo, a largo plazo puede provocar la Desarticulación de la organización.	2
BAJO	Causa daño aislado, que no perjudica a ningún componente del Área o de la organización.	1

- **Impacto de amenaza.-** grado de impacto al materializarse la amenaza. En este caso se manejan la siguiente ponderación:

Tabla 4.10 **Ponderación de impacto. Elaborado por autor.**

ALTO	La realización del hecho es inminente. No existen condiciones internas y externas que impidan el desarrollo del hecho.	3
MEDIO	Existen condiciones que hacen poco probable un hecho en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.	2
BAJO	Existen condiciones que hacen muy lejana la posibilidad de que el hecho se presente.	1

- **Calificación de riesgo.-** impacto que se refleja por la multiplicación de la probabilidad de explotación de vulnerabilidad por el impacto de amenaza. Mientras la calificación sea más alta, el riesgo es más alto y se debe dar prioridad a los controles a ser tomados por la institución.
- **Controles.-** controles a ser aplicados para mitigar el riesgo. Éstos son basados en las recomendaciones que se exponen en el acurdo 166 y las normas ISO. (Ver Tabla 3).

En la **Tabla 4.7** presenta una matriz con la identificación de activos de información con que cuenta la Superintendencia de Control del Poder de Mercado.

Tabla 4.11 **Evaluación de riesgos. Elaborado por autor.**

SCPM

EVALUACIÓN DE RIESGOS

Alto	3
Medio	2
Bajo	1

Activos	AMENAZAS	VULNERABILIDADES	Probabilidad de explotación de Vulnerabilidad	Impacto de Amenaza	Calificación Riesgo (P*I)	Control ISO 27002
Expediente	Destrucción del documento	Manipulación inadecuada	2	3	6	Gestión de activos Control de accesos
Expediente con avance de información de casos	Divulgación no autorizada	Falta de control de accesos	2	3	6	Control de accesos
Base de Datos	Eliminación no autorizada de información	Control de acceso inadecuado.	1	3	3	Control de accesos
Switch de core	Interrupción del servicio debido a fallas eléctricas	Protección inadecuada de la red eléctrica	1	2	2	Control de accesos
Servidor SRV-BDD-ORA	Fallos de hardware	Falta de gestión de mantenimiento.	1	2	2	Control de accesos
Intendente de prácticas desleales	Pérdida de confidencialidad	Falta de políticas, acuerdos de confidencialidad y normas de desvinculación de empleados	1	3	3	Gestión de activos Control de accesos
Instalaciones SCPM	Incendio	Presencia de material inflamable no autorizado.	1	3	3	Seguridad física y ambiental
Escaneado del documento	Duplicación de información	Falta de control de accesos	1	3	3	Gestión de activos Control de accesos

Documento Impreso	Perdida del documento	Inadecuada manipulación de la documentación	2	3	6	Gestión de activos
Formulario	Falta de procedimiento para tratamiento de información	Carencia de un procedimiento de uso de la documentación	2	3	6	Gestión de activos
	Uso no controlado de datos	Carencia de un procedimiento de uso de la documentación	2	1	2	Gestión de activos
		Archivador con acceso publico	3	1	3	Gestión de activos
Base de Datos	Manipulación / Corrupción de datos inadvertida	Control inadecuado de base de datos	2	3	6	Control de acceso
		Falta de política de monitoreo de logs	2	2	4	Gestión de activos Control de accesos
	Eliminación negligente de datos	Control inadecuado de base de datos	1	3	3	Gestión de activos Control de accesos
		Falta de política de control de acceso a la red	2	1	2	Gestión de activos Control de accesos
Software institucional	Uso de software por usuarios no autorizados	Administración inadecuada del aplicativo	2	2	4	Gestión de activos Control de accesos
		Inadecuado control de password	2	3	6	Gestión de activos Control de accesos
	Errores de versionamiento de aplicación	No existe política de cambio de versión	2	2	4	Políticas de Seguridad
		Equipos con ambientes locales	2	1	2	Gestión de activos Control de accesos
Servidores	Daño físico	No disponibilidad de repuestos	2	3	6	Seguridad física y ambiental
		falta de mantenimiento preventivo	2	3	6	Seguridad física y ambiental
	Robo	No existe control de acceso en datacenter	1	3	3	Gestión de activos Control de accesos

Jefe de sistemas	Perdidas de confidencialidad	Falta de políticas / normas / procedimientos para vinculación y desvinculación de empleados	2	3	6	Políticas de Seguridad Seguridad ligada a los recursos humanos
		Falta de campañas de concientización respecto a la confidencialidad de la información	3	2	6	Seguridad ligada a los recursos humanos
	Abuso de derechos de perfiles usuarios	Excesiva autoridad	3	2	6	Seguridad ligada a los recursos humanos
		No existe auditoria de sistemas	2	2	4	Políticas de Seguridad
Oficina	incendio	Falta de Sensores de Incendio	1	2	2	Seguridad física y ambiental
		Falta de Sistema contra incendio	1	2	2	Seguridad física y ambiental

4.7. Controles a ser implementados

Una vez evaluado los riesgos se tomará como referencia las políticas a ser aplicadas en consideración con los lineamientos de seguridad de información en documentos confidenciales que se enmarcan en el objeto de este proyecto.

4.7.1. Políticas de operación

En referencia a las controles presentados en la matriz de riesgos y según las normas internacionales ISO 27000 y al acuerdo 166 emitido por la Secretaría Nacional de Administración Pública, se plantean las siguientes políticas a ser aplicadas en la Superintendencia de Control del Poder de Mercado, para control de documentación confidencial en sus flujos internos.

4.7.1.1. Políticas sobre el control de acceso a los sistemas.

4.7.1.1.1. Objetivo

Establecer lineamientos y procedimientos internos para el control al acceso a la información confidencial con que cuenta la Superintendencia de Control del Poder de Mercado.

4.7.1.1.2. Generalidades

- El acceso a la información a los sistemas institucionales, será asignado de acuerdo a los roles y responsabilidades que involucra a cada servidor de la SCPM.
- La asignación de roles a los funcionarios será determinada por los líderes de cada departamento funcional, o en su defecto por parte de los coordinadores o autoridades de cada área involucrada de la SCPM.

- Se utilizará la segregación de funciones, para diferenciar las responsabilidades de cada usuario, de acuerdo a la identificación de los roles de cada proceso.
- Se evitará, bajo todo concepto, que la definición de roles genere conflictos de intereses en el acceso, control y protección de la seguridad de la información.
- Se prohíbe la creación y uso de usuarios genéricos, usuarios con privilegios de administrador o súper usuarios, para las tareas que involucren gestión de la información de los sistemas institucionales.
- Se establecerá el principio de menor privilegio para la asignación de permisos, es decir que cada funcionario contará con los mínimos privilegios que le permitan cumplir con sus funciones
- En el caso de que un funcionario requiera los permisos de acceso de un rol que no le corresponde, se deberá justificar la necesidad de acceso y en caso de asignar los permisos solicitados, estos deberán ser de carácter temporal.
- La asignación de los roles a los funcionarios es intransferible, y deberá ser actualizada de acuerdo a las necesidades institucionales.
- La definición de roles y responsabilidades con sus respectivos accesos a la información de los sistemas institucionales, deberán ser verificados y actualizados continuamente por parte de los propietarios de la información.

4.7.1.1.3. Sobre los dispositivos móviles

- La asignación de privilegios de acceso en dispositivos móviles cumplirá con los mismos principios generales establecidos en la presente política.
- Las medidas de seguridad específicas que se deberán incluir para el uso de dispositivos móviles son:
  - Encriptación de contenido.
  - Respaldos periódicos
  - Restricción de instalación de aplicaciones de terceros
  - Capacitación a los usuarios de estas tecnologías
- Las políticas referentes a dispositivos móviles, específicamente tabletas y teléfonos inteligentes, deberán ser revisadas continuamente y validadas a medida que se implementen nuevas funcionalidades en los sistemas institucionales.
- Se prohíbe el acceso a los módulos de los sistemas institucionales que no hayan sido certificados para plataformas móviles.

4.7.1.1.4. Métricas

Las métricas para medir el éxito de la implementación de esta política son:

- Número de violaciones de acceso por privilegios excesivos de los roles definidos.
- Interrupción de las actividades debido a privilegios insuficientes.

- Número de observaciones encontradas en auditorias por conflicto de intereses en los privilegios de acceso a la información institucional.

4.7.1.1.5. Herramienta

La herramienta que se utilizará para realizar este control es una herramienta de prevención de fuga de información DLP, tal como se muestra en la **Tabla 3.1**.

4.7.1.2. Políticas acerca del recurso humano.

4.7.1.2.1. Objetivos

- Definir planes de relevo y capacitación de acuerdo a información sobre el personal en puestos claves de cada institución y donde se genere y tramite información sensible.
- Actualización de antecedentes del personal que labora en la SCPM.

4.7.1.2.2. Generalidades sobre el empleo y contratación

- Todo el personal propio o contratado, que tenga acceso a la información de los sistemas institucionales, deberá cumplir con las políticas y lineamientos de seguridad de información establecidos.
- Las áreas de Talento Humano serán las encargadas de recolectar y verificar información relevante sobre los antecedentes del personal que ingresa a la institución, siempre que estas actividades no atenten contra el derecho a

la intimidad y otras leyes relacionadas. La información básica a recolectar y verificar debe incluir:

- Referencias laborales y personales
- Calificaciones académicas
- Record policial

- En caso de que el personal que tenga acceso a información confidencial sea proporcionado por una contratista o similar, se debe exigir que los términos del contrato incluyan responsabilidad en la investigación de antecedentes de sus empleados, y cumplimiento con las políticas de seguridad de información establecidos.
- Se deberá informar a todo candidato que aplique a la vinculación de cualquier cargo dentro de la institución, que la información entregada en sus hojas de vida será verificada y sometida a investigación.
- Todo el personal que ingrese y tenga acceso a información sensible de la institución, deberá suscribir acuerdos de confidencialidad de acuerdo al tipo de información que gestione en sus actividades diarias.

4.7.1.2.3. Sobre las responsabilidades de la SCPM.

La SCPM deberá asegurar que sus empleados y contratistas:

- Estén debidamente informado de sus roles y responsabilidades, antes de tener acceso a la información de los sistemas institucionales.

- Conozcan los lineamientos de seguridad de la información en las actividades que van a realizar.
- Cumplan con la normativa interna y las políticas de seguridad de la información establecidas en cada institución.

4.7.1.2.4. Conocimiento, educación y capacitación

- Todo el personal de la SCPM, y de ser necesario los contratistas, deberán recibir capacitación y actualización de conocimientos sobre seguridad de la información.
- La capacitación de seguridad de la información, deberá incluir la inducción para conocimiento y uso de las políticas y normas de la SCPM.
- Se debe verificar que el personal asignado a tareas de seguridad de la información cumpla con los requisitos de especialización y formación de acuerdo a los roles y responsabilidades asignados, caso contrario deberán incluirse en los planes de capacitación de la SCPM.
- La SCPM debe impulsar iniciativas de concienciación, por parte de todos los empleados, sobre la importancia de la seguridad de la información en todas las actividades institucionales.

4.7.1.2.5. Sobre la terminación de la relación laboral o cambio de funciones

- Toda terminación de relación laboral deberá considerar los acuerdos de confidencialidad establecidos, y se deberá implementar los métodos de control que garanticen su

cumplimiento durante el tiempo posterior a la separación que establezca el acuerdo.

- El área de Talento Humano, encargada de gestionar la terminación de la relación laboral, deberá trabajar en conjunto con el área de seguridad para manejar los aspectos relevantes con la seguridad de la información.
- La salida de personal deberá considerar la desvinculación de los permisos de acceso de manera inmediata o incluso de forma previa a la notificación, verificando los roles y responsabilidades asignados o relación con grupos de acceso. La desvinculación de los permisos no implica que sean eliminados de registros o históricos ya que esta información puede ser de utilidad en procesos de auditoría o similares.
- Se deberá informar a todo el personal relacionado, sobre la salida o separación de funcionarios para que se evite enviar o compartir información con la persona que se va.
- El cambio de funciones o puesto dentro de la SCPM, deberá ser considerado de forma similar a la terminación en el sentido de los permisos de acceso a la información, es decir que se deberá deshabilitar todo permiso actualmente asignado y posteriormente se procederá a asignar los nuevos permisos según corresponda, esta también es una consideración válida para los procesos de auditoría.
- Se debe identificar los puestos claves y el personal asignado a dichos puestos, para establecer planes de relevo o

reemplazo en caso de ausencia de dicho personal, ya sea por separación definitiva o rotación.

4.7.1.2.6. Métricas

- Cantidad de perfiles y antecedentes verificados por parte de Talento Humano.
- Cantidad de personal debidamente capacitado de acuerdo a las necesidades identificadas.
- Cantidad de puestos clave identificados, cuyo personal asignado no cuenta con reemplazo en caso de ausencia o separación.

4.7.1.3. Política sobre el manejo de información confidencial.

4.7.1.3.1. Objetivos

- Definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida.
- Asegurar el cumplimiento de regulaciones y leyes aplicables a las entidades del estado ecuatoriano.

4.7.1.3.2. Alcance

Ésta política aplica para todo el personal que labora en Superintendencia de Control de Poder de Mercado, sean éstos directivos, funcionarios, contratistas, consultores, pasantes, personal temporal, etc.

4.7.1.3.3. Definiciones

- **Información pública.-** esta es expuesta para que todas las personas que laboran en la SCPM puedan disponer de la misma.
- **Información restringida.-** esta información debe estar expuesta para el personal que labora en la SCPM, pero no expuesta al público general.
- **Información confidencial.-** esta información debe estar expuesta sólo a personal designado en la SCPM para valoración y tratamiento de la misma. Nunca debe ser expuesta a personal externo de la Institución.

4.7.1.3.4. Generalidad

Se debe considerar la sensibilidad de los datos que residen en los sistemas de información de la SCPM para el debido control y acceso.

4.7.1.3.5. Aspectos generales

- Todo documento, carpeta, y otros medios de almacenamiento que contienen información restringida o confidencial debe ser ubicada en áreas protegidas. Estos medios de almacenamiento de información nunca deben ser ubicados en un lugar donde visitantes pueda tener acceso a ellos.
- Los medios de almacenamiento de información que contienen información restringida o confidencial debe ser guardada en un área segura todo el tiempo, la misma debe ser definida por el área de seguridad de la SCPM.

- Las computadoras portátiles (“laptops”) y otros dispositivos portátiles (tales como memoria USB / pendrive, etc.) que contiene información de la SCPM, debe tener instalado software de cifrado (“encryption”) y si no está siendo utilizada o no está en la posesión directa del usuario asignado, debe estar asegurada físicamente.
- Toda información de respaldo de datos (“backup”) enviado o almacenado en medios de datos (por ejemplo. CD, DVD, cintas magnéticas, discos ópticos, etc.) debe ser protegido y debe ser manejado según los procedimientos vigentes de la SCPM.
- Las infracciones de esta política pueden tener como resultado acciones disciplinarias conforme a políticas y procedimientos disciplinarios vigentes en la SCPM.

4.7.1.3.6. Sobre el manejo de información en estaciones de trabajo

- Todos los computadores deben ser asegurados cuando el área de trabajo esté desocupada o desatendida. El área de seguridad será responsable de aplicar un mecanismo automático para imponer esta práctica.
- Todo documento, carpeta, y otros medios de almacenamiento que contienen información restringida o confidencial debe ser retirada del escritorio y asegurada en una ubicación segura dentro del computador. El área de seguridad será responsable de aplicar un mecanismo para imponer esta práctica.

- Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información restringida o confidencial dentro de sus accesos asignados.
- Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible.
- Las contraseñas sólo pueden ser utilizadas por la persona a quién se le asignó ésta responsabilidad de acceso.
- Los informes o documentación impresa que contienen información restringida o confidencial deben ser retirados inmediatamente de las impresoras. No se debe dejar ningún tipo de documento de este tipo sobre las bandejas de impresión.
- Al momento de desechar, los documentos restringidos o confidenciales deben ser destruidos en equipos de destrucción de papel.
- Los controles de acceso y monitoreo deben ser aplicados en áreas de oficina e instalaciones de almacenaje donde resida información restringida o confidencial.

4.7.1.3.7. Proceso de notificación

En eventos los cuales información restringida o confidencial es extraviada o es divulgada a entidades no autorizadas o si este acontecimiento incluye pérdida de cualquier equipo, medio electrónico de almacenamiento o componente

tecnológico, se debe notificar inmediatamente al área de seguridad de la SCPM.

4.7.1.3.8. Medidas disciplinarias

- Las sanciones aplicables al personal, de acuerdo a la ocurrencia o severidad de la violación o infracción a esta política se regirá por lo establecido las leyes y normativas vigentes de la SCPM.
- La SCPM tiene la facultad de aplicar la sanción más severa, en este caso la desvinculación directa del personal, en aquella ocasión en que la gravedad o seriedad de la infracción no amerite permitir que se repita en una futura ocasión.

4.7.1.3.9. Métricas

- Cantidad de infracciones detectadas por el área de seguridad.
- Cantidad de sanciones aplicadas a personal que labora en la SCPM.

4.7.1.3.10. Herramienta

La herramienta que se utilizará para realizar este control es una herramienta de prevención de fuga de información DLP, tal como se muestra en la **Tabla 3.1**.

4.7.2. Documentación

La documentación presentada como normativa de seguridad entrará en vigencia desde el momento en que éste modelo sea aprobado como documento técnico de seguridad informática por las autoridades correspondientes de la Superintendencia de

Control del Poder de Mercado. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la institución, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red Institucional.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

- La seguridad de la información no es un producto que se pueda adquirir como un paquete o software para su implementación, por lo tanto la institución que requiere contar con esta característica debe estar dispuesta a seguir los procedimientos y recomendaciones que implica la implantación de este modelo.
- Se requiere contar con herramientas informáticas que permitan gestionar de manera correcta el uso de aplicaciones informáticas.
- La falta de un modelo de gestión de seguridad de la información en una institución, imposibilita gestionar los riesgos asociados debido al desconocimiento de amenazas o vulnerabilidades y los métodos adecuados para tratarlas.
- El diseño y utilización de un modelo de gestión de seguridad de la información, permitirá la estandarización de procesos y el cumplimiento con regulaciones como el acuerdo ministerial 166, emitido por la Secretaría Nacional de Administración Pública.
- El acuerdo 166 y la norma ISO/IEC 27002 pueden ser usados para el diseño de un modelo de gestión de seguridad de la información que establezca directrices que soporten las metas corporativas o de negocio y que se complemente con mejores prácticas ampliamente aceptadas por la industria de Tecnologías de Información.
- Las directrices expuestas en el presente modelo, es un elemento útil para trasladar las metas corporativas en aspectos tecnológicos u organizacionales,

caracterizando un modelo de gestión de seguridad de la información basado en: políticas, procesos, estructura organizativa, cultura organizacional, información, servicios-infraestructura y personas con sus habilidades.

- La infraestructura tecnológica con que cuenta actualmente la Superintendencia de Control del Poder de Mercado no se encuentra en un nivel óptimo para el tratamiento de información confidencial.
- La estructura organizacional de la Superintendencia de Control del Poder de Mercado, no cuenta con un área de seguridad de la información; área fundamental para tratamiento de casos relacionados con fuga de información.
- El análisis de riesgo levantado en el presente proyecto, permitió el análisis de puntos débiles y vulnerabilidades que deben ser cubiertas en la Superintendencia de Control del Poder de Mercado para corregir el tratamiento de información confidencial tratada en la misma.
- La necesidad de la adopción de un modelo de gestión de la seguridad de la información para tratamiento de documentación sensible, es primordial para corregir amenazas y vulnerabilidades dentro de las instituciones.
- La propuesta del modelo de gestión de Seguridad de la Información para la Superintendencia de Control del Poder de Mercado recoge y concreta las recomendaciones de las normas utilizadas para seguridad de la información en tratamiento de información confidencial.
- Los principios, políticas y marcos de referencia son el catalizador o elemento principal sobre el cual se debe diseñar los modelos de gestión de seguridad de la información, debido a que establecen los lineamientos para el cumplimiento de normas y políticas institucionales.

- El éxito de toda iniciativa de seguridad de la información está relacionada con el apoyo y conocimiento de personal directivo de cualquier institución que sea parte de la adopción de éstas prácticas.
- Los beneficios del modelo de gestión de seguridad de la información relacionados con los procesos implementados en la Superintendencia de Control del Poder de Mercado son:
    - Cumplimiento con requerimientos de normativa, regulación y acuerdos ministeriales.
    - Reconocimiento y protección de información crítica de los procesos implementados.
    - Definición de roles y responsabilidades para gestión y tratamiento de información confidencial dentro de la Superintendencia de Control del Poder de Mercado.
    - Establecimiento de procedimientos clave para el tratamiento de información confidencial dentro de la Superintendencia de Control del Poder de Mercado.

5.2. Recomendaciones.

- Debe existir un compromiso total por parte de personal directivo y cada uno de los funcionarios que laboren en una institución, para poder tener éxito en la implementación de un sistema de seguridad de la información.
- Siempre se debe estar pendiente de las posibles amenazas que pueden estar asechando a los activos de las instituciones; en este caso siempre se debe considerar el monitoreo constante de los flujos y procesos relacionados con la documentación institucional de las organizaciones.

- Realizar un levantamiento adecuado de los activos con que cuentan las instituciones, es primordial para poder darle un tratamiento adecuado alineado a los objetivos institucionales.
- Se debe considerar en el presupuesto laboral de las instituciones, la capacitación del personal en temas relacionados con seguridad de la información.
- Incluir un análisis de riesgos en toda la información confidencial que se genere dentro de la Superintendencia de Control del Poder de Mercado, para poder aplicar controles adecuados y gestionar acciones oportunas en caso de contingencias.
- Evitar iniciativas aisladas para tratamiento de seguridad de la información confidencial que se genere dentro de la Superintendencia de Control del Poder de Mercado, para que éstas no generen un problema de seguimiento de posibles amenazas que se pueden presentar acerca de este tema.
- Identificar e incluir las necesidades de todas las partes interesadas en las iniciativas de seguridad de la información que se generen dentro de la Superintendencia de Control del Poder de Mercado.

BIBLIOGRAFÍA

Departamento de Seguridad en Computo/UNAM-CERT. (01 de 10 de 2009). *¿Cómo crear contraseñas seguras?* . Obtenido de Usuario Casero: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=185

Encriptación. (12 de 05 de 2013). Obtenido de Tipos de encriptación: http://4esobglr.blogspot.com/2013/05/tipos-de-encriptados.html

IES San Juan Bosco. (01 de 01 de 2015). *Sistemas biométricos*. Obtenido de Seguridad de los sistemas biométricos: http://dis.um.es/~lopezquesada/documentos/IES_1112/SAD/curso/UT3/ActividadesAlumnos/grupo7/Enlaces/BIOMETRICO.html

Ingeniería SPS. (10 de 02 de 2015). Obtenido de SGSI "Sistema De Gestión De Seguridad De La Información": http://ingenieriasps.com/ing/index.php/sgsi/auditoriaiso27001menu

Iso 27000. (23 de 09 de 2014). Recuperado el 23 de 09 de 2014, de http://www.iso27000.es

ISO 27000.ES. (10 de 01 de 2005). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/

ISO 27000.es. (31 de 07 de 2012). *El portal de ISO 27001 en Español*. Obtenido de ¿Qué es un SGSI?: http://www.iso27000.es/sgsi.html

iso27002.es - El Anexo de ISO 27001 en español. (10 de 01 de 2013). *iso27002.es - El Anexo de ISO 27001 en español*. Obtenido de ISO 27002: http://www.iso27002.es/

Mejía, D. (12 de 05 de 2015). Esquema de personal de seguridad. *Autoría Propia*. Quito, Pichincha, Ecuador.

Mejía, D. (12 de 05 de 2015). Modelo de Seguridad. Quito, Pichincha, Ecuador.

Secretaría Nacional de Administración Pública. (23 de 09 de 2013). *Acuerdo Nro. 166.* Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf

Secretaría Nacional de Administración Pública. (23 de 09 de 2014|). Recuperado el 20 de 08 de 2014, de http://www.administracionpublica.gob.ec/

Superintendencia de Control del Poder de Mercado. (23 de 09 de 2014). Recuperado el 23 de 09 de 2014, de www.scpm.gob.ec

Superintendencia de Control del Poder de Mercado. (12 de 05 de 2015). *Superintendencia de Control del Poder de Mercado*. Obtenido de SCPM MIsión: http://www.scpm.gob.ec/scpm-mision/

The ISO 27000 Directory. (02 de 10 de 2013). *The ISO 27000 Directory*. Obtenido de An Introduction to ISO 27001, ISO 27002....ISO 27008: http://www.27000.org/

The ISO 27000 Directory. (10 de 01 de 2013). *The ISO 27000 Directory*. Obtenido de Introduction To ISO 27002 (ISO27002): http://www.27000.org/iso-27002.htm

Universidad Politécnica de Madrid. (14 de 01 de 2015). *Tarjetas Inteligentes*. Obtenido de Tarjetas Inteligentes: http://www.upm.es/institucional/Estudiantes/OrdenacionAcademica/CarneUniversitario/e58f4105a0052210VgnVCM10000009c7648aRCRD